Y2K MYTHS AND REALITIES

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY

OF THE

COMMITTEE ON SCIENCE

AND THE

SUBCOMMITTEE ON
GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON
GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

NOVEMBER 4, 1999

Science Serial No. 106–61
Government Reform Serial No. 106–67

Printed for the use of the Committee on Science and the Committee on Government Reform

U.S. GOVERNMENT PRINTING OFFICE

61–629 WASHINGTON : 2000

COMMITTEE ON SCIENCE

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

SHERWOOD L. BOEHLERT, New York
LAMAR SMITH, Texas
CONSTANCE A. MORELLA, Maryland
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
JOE BARTON, Texas
KEN CALVERT, California
NICK SMITH, Michigan
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
DAVE WELDON, Florida
GIL GUTKNECHT, Minnesota
THOMAS W. EWING, Illinois
CHRIS CANNON, Utah
KEVIN BRADY, Texas
MERRILL COOK, Utah
GEORGE R. NETHERCUTT, JR., Washington
FRANK D. LUCAS, Oklahoma
MARK GREEN, Wisconsin
STEVEN T. KUYKENDALL, California
GARY G. MILLER, California
JUDY BIGGERT, Illinois
MARSHALL "MARK" SANFORD, South Carolina
JACK METCALF, Washington

RALPH M. HALL, Texas, *Ranking Minority Member*
BART GORDON, Tennessee
JERRY F. COSTELLO, Illinois
JAMES A. BARCIA, Michigan
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
LYNN N. RIVERS, Michigan
ZOE LOFGREN, California
MICHAEL F. DOYLE, Pennsylvania
SHEILA JACKSON LEE, Texas
DEBBIE STABENOW, Michigan
BOB ETHERIDGE, North Carolina
NICK LAMPSON, Texas
JOHN B. LARSON, Connecticut
MARK UDALL, Colorado
DAVID WU, Oregon
ANTHONY D. WEINER, New York
MICHAEL E. CAPUANO, Massachusetts
BRIAN BAIRD, Washington
JOSEPH M. HOEFFEL, Pennsylvania
DENNIS MOORE, Kansas
Vacancy

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. MCINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
HELEN CHENOWETH-HAGE, Idaho
DAVID VITTER, Louisiana

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee
JANICE D. SCHAKOWSKY, Illinois

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
DAVID A. KASS, *Deputy Counsel and Parliamentarian*
CARLA J. MARTIN, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois
THOMAS M. DAVIS, Virginia
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
MATTHEW RYAN, *Senior Policy Director*
BONNIE HEALD, *Communications Director/Professional Staff Member*
CHIP AHLSWEDE, *Clerk*
TREY HENDERSON, *Minority Professional Staff Member*

CONTENTS

NOVEMBER 4, 1999

Y2K MYTHS AND REALITIES

THURSDAY, NOVEMBER 4, 1999

HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY, COMMITTEE ON GOVERNMENT REFORM, JOINT WITH THE SUBCOMMITTEE ON TECHNOLOGY, COMMITTEE ON SCIENCE,

Washington, DC.

The Subcommittees met, pursuant to call, at 2:15 p.m., in room 2318, Rayburn House Office Building, Hon. Constance A. Morella (Chairwoman of the Subcommittee on Technology) presiding.

Chairwoman MORELLA. I am going to gavel the joint subcommittees' hearing to order.

You just heard the beeper; we're going to have a series of about four, probably maybe even five votes. But I thought I would give an opening statement and then return right after the votes. There is also a markup taking place in Government Reform, which is where our co-chair is right now, and that is why you do not have the members here. They will return. But I will at least comment on what we are here today to listen to and what the topic is of the meeting.

I want to welcome all of you to the House's Y2K Working Group, that is comprised of the Science Committee's Technology Subcommittee and the Government Reform Committee's Government Management, Information, and Technology Subcommittee.

With the anticipated adjournment of the first session of this 106th Congress looming before us, this hearing is expected to be the culmination of our House Y2K Working Group efforts before the January 1, 2000, deadline.

It is sometimes hard to believe that we have focused on this issue ever since the spring of 1996. When our two subcommittees held the first congressional hearings 3½ years ago on the then little publicized year 2000 computer problem, the millennium bug seemed to be more suited to the realm of exterminators than Congress. But our Y2K review revealed some troubling news. At that time, our Nation was simply not moving forward with the required dispatch to effectively respond to the devastating effects of the "mother" of all computer glitches, potentially crippling vital Government functions, critical industry performance, and our robust economy.

We in Congress attempted to step up to the plate by raising awareness about the problem and by pushing Federal agencies and private industry toward immediate corrective measures. We did this through a series of comprehensive hearings, vigilantly exer-

cised our oversight authority, and enacted laws that required the creation of a national Federal strategy and prohibited the purchase of Federal information technology that was not Y2K compliant.

It was clear, however, that despite our congressional powers, the legislative branch alone was ill-suited to lead our Nation's Y2K efforts. We desperately needed the help of the President's executive powers. We were frustrated by what seemed to be the lack of leadership. It was clear to us that without greater urgency and aggressive agency management, Federal agencies were at risk of being unable to provide services or to perform functions that are critical to its mission and vital to the American public.

We spent a year urging the President to personally embrace the need for Federal action and to appoint a Y2K czar to oversee the Nation's public and private sector initiatives, until he finally appointed a very capable man, who is here today, John Koskinen, to chair the Year 2000 Conversion Council. Given the late start in his appointment, John, who was lured out of retirement to take on this herculean task, obviously had his work cut out for him. And while we have not necessarily agreed on all aspects of our Nation's Y2K strategy, I want to say to John that your extremely competent achievements, performed with such a high level of professional dedication and commitment to public service, really do deserve recognition.

Since John's appointment, we in Congress have successfully worked together to require greater Federal and private sector disclosures, provide a special Federal appropriation solely for Y2K efforts, raise Y2K awareness throughout the country, and enact laws to improve Y2K readiness, and to curb the number of frivolous glitch-related law suits.

Yet, as we now move toward the remaining 50 days before the unforgiving and immovable Y2K deadline, Americans still have a number of questions about how, in the midst of all their millennium celebrations, they will be affected, if at all, by the year 2000 problem. We know the American people are counting on us.

This hearing is designed to respond to some of those questions. I am pleased that we have a distinguished panel of witnesses that seek to help us provide some of those answers today.

Finally, before I turn to our ranking member of the Technology Subcommittee, I want to thank, on behalf of both of us including Chairman Horn, who will be with us later, to all of our fellow colleagues on the House Y2K Working Group, I want to thank them for their leadership, support, and participation. It is also important to note that our Y2K efforts have been bipartisan. I want to commend our ranking members, Mr. Barcia of Michigan, who is here with us, Mr. Turner of Texas, Mr. Gordon of Tennessee, Mrs. Maloney of New York, Mr. Kucinich of Ohio.

And now I would be very happy to recognize the Ranking Member of the Technology Subcommittee, Mr. Barcia, for any opening remarks before we go vote.

[The prepared statement of Hon. Constance A. Morella follows:]

Opening Statement of
Congresswoman Constance A. Morella

Chairwoman, Technology Subcommittee
House Science Committee

Y2K Myths and Realities: Responding to the Questions of the American Public With 50 Days Remaining Until January 1, 2000

Final oversight hearing on the status of the Year 2000 computer problem

Thursday, November 4, 1999

Welcome to today's hearing of the House Y2K Working Group, comprised of the Science Committee's Technology Subcommittee and the Government Reform Committee's Government Management, Information and Technology Subcommittee.

With the anticipated adjournment of the first session of this 106th Congress looming before us, this hearing is expected to be the culmination of our House Y2K Working Group efforts before the January 1, 2000 deadline.

It is sometimes hard to believe that we have focused on this issue ever since the spring of 1996.

When our two subcommittees held the first Congressional hearings 3½ years ago on the-then little publicized Year 2000 computer problem, the millennium bug seemed to be more suited to the realm of exterminators than Congress.

But our Y2K review revealed some troubling news.

At that time, our nation was simply not moving forward with the required dispatch to effectively respond to the devastating effects of the mother of all computer glitches – potentially crippling vital government functions, critical industry performance, and our robust economy.

We, in Congress, attempted to step up to the plate by raising awareness about the problem and by pushing federal agencies, and private industry toward immediate corrective measures.

We did this through a series of comprehensive hearings, vigilantly exercised our oversight authority, and enacted laws that required the creation of a national federal strategy and prohibited the purchase of federal information technology that was not Y2K complaint.

It was clear, however, that despite our Congressional powers, the legislative branch alone was ill-suited to lead our nation's Y2K efforts.

We desperately needed the help of the President's executive powers and were frustrated by his lack of leadership.

It was clear to us that without greater urgency and aggressive agency management, federal agencies were at risk of being unable to provide services or to perform functions that are critical to its mission and vital to the American public.

We spent a year urging the President to personally embrace the need for federal action and to appoint a Y2K Czar to oversee the nation's public and private sector initiatives – until he finally appointed John Koskinen to chair the Year 2000 Conversion Council.

Given the late start in his appointment, John, who was lured out of retirement to take on this Herculean task, obviously had his work cut out for him.

While we have not necessarily agreed on all aspects of our nation's Y2K strategy, I want to say to John, that your extremely competent achievements performed with such a high level of professional dedication and commitment to public service deserves recognition.

Since John's appointment, we, in Congress, have successfully worked together to require greater federal and private sector disclosures, provide a special federal appropriation solely for Y2K efforts, raise Y2K awareness throughout the country, and enact laws to improve Y2K readiness and to curb the number of frivolous glitch-related lawsuits.

Yet, as we now move towards the remaining 50 days before the unforgiving and immovable Y2K deadline, Americans still have a number of questions about how, in the midst of all their millennial celebrations around the world, they will be affected, if at all, by the Year 2000 problem.

We know the American people are counting on us.

This hearing is designed to respond to some of those questions and I am pleased that we have a distinguished panel of witnesses that seek to help us provide some of those answers today.

Finally, before I turn to the Co-chair of this hearing, I want to thank, on behalf of both of us, all of our fellow colleagues of the House Y2K Working Group for their leadership, support, and participation.

It is also important to note that our Y2K efforts have been bipartisan with several Ranking Members, over the years, Mr. Barcia of Michigan, Mr. Turner of Texas, Mr. Gordon of Tennessee, Ms. Maloney of New York, and Mr. Kucinich of Ohio.

I now recognize the Co-Chair and my co-collaborator, my friend and a leader of our Congressional Y2K efforts, the distinguished gentleman from California, the Chairman of the Government Management, Information and Technology Subcommittee, Mr. Horn.

Mr. BARCIA. Thank you, Chairwoman Morella. I want to return the compliment and thank you for the leadership and the bipartisan nature in which you have conducted the hearings of this subcommittee, and the tremendous amount of energy and time that you have invested in this Y2K issue and its importance to the citizens across the country.

I want to join my colleagues on the subcommittee in welcoming our distinguished panel to this last hearing of the year 2000 computer bug.

Over the past 3 years, we have held hearings on almost every aspect of the Y2K problem; on Federal agencies' efforts, international issues, State and local government efforts, the impact on industry, and liability. Although confident with the strides made by Federal agencies, we continue to be hampered in our assessment of the impact of the year 2000 problem on State and local governments and industry because there is still a lack of factual information on Y2K readiness.

I urge our panelists today to provide us with as much specific information as possible about the overall level of Y2K readiness in the United States and abroad, if you can. If we are to calm public fears, we must provide the public with facts.

This series of hearings has served to educate the public about the magnitude and scope of the Y2K problem. And although it has been my experience that most people are aware of the Y2K issue, they still do not have a good understanding of its potential impact or lack of impact. I am concerned because, unless we get the message out, the level of public fear could rise.

What could be the single largest public awareness announcement, a November 21st made for television movie, entitled, "Y2K: The Movie." According to news reports, this movie has the U.S. Government grounding all airplanes, the Eastern seaboard experiencing a major power outage, and even worse problems yet to come. In the absence of facts, what is designed to be entertainment could achieve the saddest effect.

As this is the last hearing, I would like to commend Mr. Joel Willemssen and the staff of GAO for the outstanding work that they have done during the past 3 years. I would also like to commend Mr. Koskinen for the coordination role his office has provided in the administration's Y2K efforts. And, of course, finally, I want to thank the witnesses for appearing before us. I look forward to hearing your comments.

Thank you, Madam Chair.

[The prepared statements of Hon. Debbie Stabenow and Hon. Jim Turner follow:]

SUBCOMMITTEE ON TECHNOLOGY

HEARING ON Y2K MYTHS AND REALITIES: RESPONDING TO THE QUESTIONS OF THE AMERICAN PUBLIC WITH 50 DAYS REMAINING UNTIL JANUARY 1, 2,000

Opening Statement of Congresswoman Debbie Stabenow
of the 8th District, State of Michigan

November 4, 1999

Madame Chairwoman, Ranking Member Barcia, it is hard to believe we have reached the end of our Y2K hearings. I appreciate the thoroughness with which the Subcommittee has approached this important and unique topic, and look forward to our final discussion today. I am interested in hearing the current assessment of our Y2K preparedness, and I hope we dedicate a good portion of our time to the question of state preparedness and how problems at that level may impact federal programs. As we all know, the states have a role in administering many federal programs, such as LIHEAP, Medicaid, and Food Stamps. How will the federal government aid in restoring these services if complications occur?

I would also like to address this afternoon the recent media reports that federal law enforcement agencies are recommending that more attention be given to possible violent outbursts by militia and other groups surrounding the beginning of the new millennium. Do we know how extensive such activities are likely to be and how serious? At the same time, I think we also need to remind ourselves of the important role government officials can play in informing the public concerning what to expect on January 1. Practical preparations, such as storing extra food and water and a little extra cash, should not give way to panic. This is a role I think the President's Y2K Council has performed well, and I urge us all to maintain this effort for the next fifty days.

Madame Chairwoman, I would like to again thank the Subcommittee for its rigorous treatment of this subject matter, as well as our panelists for their continued dedication to helping us with these topics. With less than two months to go, I will welcome the passing of this much anticipated event.

STATEMENT OF THE HONORABLE JIM TURNER
JOINT HEARING ON "Y2K MYTHS AND REALITIES"
11/04/99

Thank you. For more than three and a half years, this Subcommittee along with the Technology Subcommittee of the Science Committee have held congressional hearings on the Year 2000 computer challenge, focusing on virtually every facet of the computer problem. These hearings have included such high risk Y2K areas as the Global Positioning System (GPS), international air travel, and the healthcare industry.

Due in large part to the hard work of Chairman Horn, Chairwoman Morella, the Administration, and these committees, we believe the federal government's computer systems are ready to successfully operate in the new millennium. I want to commend the committees and the agencies for their diligence in meeting this challenge. According to John Koskinen, chairman of the President's Council on Year 2000 Conversion, the council has a "high degree of confidence" that many major domestic areas are Y2K compliant. However, nobody really knows for sure what will happen on January 1, 2000.

Therefore, I think it is appropriate that the House Y2K Task Force's final hearing before January 1, 2000, should focus on the public's reaction to Y2K's myths and realities. Because we are dealing with a new problem of a such a large magnitude, we should, as I have mentioned before, always expect the unexpected. Such a situation is ripe for pranksters, hackers, frauds, and others who seek to mislead the public on what might happen due to the Y2K problem. We all know that their has already been a lot of propaganda and confusion over what might happen as a result of Y2K.

I understand that a movie on Y2K will be released shortly which capitalizes on this fear and portrays a world in chaos due to computer problems associated with the rollover. Misinformation about this subject could potentially cause serious problems. For example, it is my understanding that last week IBM announced that sales of personal computers were down as consumers and businesses are not buying PCs until after January 1, 2000. Consequently, IBM's stock lost value.

At a hearing on this topic last week, I suggested that the agencys' put together some type of centralized communication center to educate the public on Y2K and correct any misinformation that pranksters or hackers may spread. I even went as far as to recommend that a high credible figure such as a "Walter Cronkite type" be employed to serve as spokesman for this issue. We have an obligation to educate and inform society on Y2K, and I will be anxious to learn what the agencys' have planned to stop misinformation.

Today, we will discuss the federal government's progress and challenges that remain in correcting its systems. There are several significant areas that we still need to be concerned about, including the status of local governments, healthcare, education, and small businesses. It has been noted that some organizations are not paying appropriate attention to the Y2K problem or are adopting a "wait and see" approach.

Again, I would like to thank the chairs and the witnesses for their focus and hard work, and I look forward to a productive hearing.

Chairwoman MORELLA. Thank you, Mr. Barcia.

As you probably know from the timing, we have got to go over to vote. We have got about 6 minutes, if even that, before the vote. There are going to be about five procedural votes.

Mr. Koskinen, I know you must leave here shortly. So what I will do is go over and vote and, if there is a 15 minute interval, come back so we can hear some of your oral testimony. Will there be somebody else here who could also respond to any questions we may have when you have to leave?

Mr. KOSKINEN. Well, with all these wonderful witnesses, someone will know. But there is no one else from my office.

Chairwoman MORELLA. And you have a written testimony for us, too, which will be part of the record.

So I shall return after our first vote when we have a 15 minute interval. For the rest of you, it will probably be about three-quarters of an hour before we reconvene fully the hearing beyond Mr. Koskinen. Thank you.

[Recess.]

Chairwoman MORELLA. I am going to reconvene the joint hearing.

I am going to ask Mr. Koskinen and Mr. Willemssen, in the tradition of the Science Committee, if they would please stand and raise their right hands. Do you swear that the testimony that you are about to give is the truth, the whole truth, and nothing but the truth?

[Witnesses respond in the affirmative.]

Chairwoman MORELLA. The record will show an affirmative response.

Mr. Koskinen, we are delighted that we will have you give us your comments at this very last meeting of the year 1999 of the Joint Y2K Working Group.

TESTIMONY OF HON. JOHN KOSKINEN, SPECIAL ASSISTANT TO THE PRESIDENT, CHAIRMAN, PRESIDENT'S COUNCIL ON YEAR 2000 CONVERSION; AND JOEL C. WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, U.S. GENERAL ACCOUNTING OFFICE

Mr. KOSKINEN. Thank you. Good afternoon, Chairwoman Morella. I am pleased to appear before you today to discuss the year 2000 issue, or Y2K, as it is known. Let me begin by thanking the Chairwoman for her very kind comments which I genuinely appreciate.

The subcommittees themselves deserve great credit for their continuing interest in the Y2K issue. Your efforts have helped to increase the visibility of this important challenge within the Federal Government and the country as a whole.

With your permission, I will submit my full statement for the record and summarize it here.

Chairwoman MORELLA. Hearing no objections, so ordered.

Mr. KOSKINEN. In keeping with the title for this hearing, let me begin with what I believe are some of the more important myths and realities regarding the Y2K issue.

One of the more troubling Y2K myths is the notion that January 1 is a seminal date on which everything, or nothing, Y2K-related

will occur. As you know, year 2000 challenges can happen any time a computer that is not Y2K-compliant comes into contact with a year 2000 date, before or after January 1. In fact, a number of businesses and governments have already had to use year 2000 dates in their automated operations. Information technology professionals are well aware that the Y2K challenge is not limited to January 1 and they will be monitoring systems well into the New Year for flaws in billing and financial cycles and possible slow degradations in service.

Another important myth deals with the reporting of Y2K readiness data. It goes something like this: Self-reported Y2K information is not valid since people will not voluntarily report problems, so virtually everything we have heard in terms of industry and Government progress reports cannot be believed. This is not true for several reasons. Most organizations have structures in place whereby independent authorities have been reviewing the results of Y2K testing. In some industries, such as electric power, Government agencies have conducted selected audits of the reported information and found no major discrepancies. And, most importantly, the industry surveys done for the President's Council have been conducted pursuant to the Year 2000 Information and Readiness Disclosure Act provisions, which the Congress passed at our urging last year. This act guarantees individual companies that their responses to these surveys will be treated confidentially, such substantially increases the likelihood of candid responses.

In the interest of time, let me now move to a discussion of the operation of the Council's Information Coordination Center, or ICC, as it is known.

The ICC will be the Federal Government's central point for coordinating a wide range of information on system operations and events related to the Y2K transition that will be collected by Government emergency centers and the private sector. The ICC will gather information about system operations in Federal agencies; among State, local, and tribal governments; in critical areas of the private sector; and internationally.

To accomplish this task, we are relying to the greatest extent possible on existing structures and expertise. Domestically, information on systems operations will be collected by the States and provided through normal channels to FEMA which will review the reports and pass them on to the ICC. In addition, the ICC will receive reports from national information centers established, many for the first time, by the private sector. The status reports will be provided to appropriate lead agencies. We presently have agreements with the electric power, banking, finance, telecommunications, oil, gas, airline, pharmaceutical, and retail industries to operate information centers during the rollover period and to share information on the status of their members with the ICC.

The ICC will receive international status reports from the State Department, the Defense Department, the intelligence agencies, private sector information centers, and national Y2K coordinators around the world. In addition, the ICC will work with the National Infrastructure Protection Center and Computer Emergency Response teams here and around the world to monitor unauthorized intrusions into systems.

Information gathered by the ICC will be the basis for complete, regularly updated national and international status reports that will be provided to all Federal agencies and organizations sharing information with the center. These reports will help agency decision makers determine what, if any, Federal actions are appropriate in response to Y2K-related difficulties. Status reports will also be provided on a regular basis to the Congress and to the public.

As I mentioned earlier, based on available information, we do not believe the Y2K issue will create significant problems in the United States. But no one can rule out the possibility that there will be temporary disruptions in some services. This week we published "Y2K and You," an information booklet on the Y2K issue as well as a "Y2K Preparedness Checklist," which I am submitting as part of the record. Our suggestions include preparing for the long holiday weekend by having at least a 3 day supply of food and water, keeping copies of important financial records before and after January 1, 2000, and checking with manufacturers to make sure that home electronic equipment is Y2K ready.

Perhaps most importantly, whatever people are going to do to prepare, they should do it early. If everyone waits until the last moment to take even modest precautions, supply systems could be overwhelmed.

When I appeared before you in January of this year, I closed by saying that overreaction by the public to real or perceived Y2K risks was in some ways our greatest challenge. I still believe that. On the other hand, our goal is not public complacency. All of us need to encourage the public to take the appropriate steps to be ready for the date change. As I said in January, the way to achieve this delicate balance is to provide people with as much information as possible about Y2K readiness efforts, the good and the bad.

Thank you for the opportunity to continue this process of information sharing here today. I would be pleased to answer any questions you may have now or in the future.

[The prepared statement of Mr. Koskinen follows:]

STATEMENT OF JOHN A. KOSKINEN
CHAIRMAN
PRESIDENT'S COUNCIL ON YEAR 2000 CONVERSION
BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY
OF THE COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT
AND THE
SUBCOMMITTEE ON TECHNOLOGY
OF THE COMMITTEE ON SCIENCE
U.S. HOUSE OF REPRESENTATIVES

November 4, 1999

Good afternoon, Chairwoman Morella, Chairman Horn and members of the subcommittees. I am pleased to appear before you today to discuss the Year 2000 (Y2K) issue.

I would like to start by thanking the subcommittees for your continuing interest in the Y2K issue. Your efforts have helped to increase the visibility of this important challenge within the Federal Government and the country as a whole.

I think it is altogether fitting that, with 57 days until January 1, we are gathered here to discuss the American public's questions about Y2K that are reflected in the ambitious set of objectives you have announced for today's hearing. I will not attempt to cover all of the topics outlined in the objectives, as you will hear today from others with expertise in several of these areas, but I would like to address what I believe are some of the more important myths and realities regarding the Y2K issue. I will also discuss the Federal Government's plans for the date rollover as well as steps individuals can take to prepare for the century date change.

Y2K Myths and Realities

As public awareness of the Y2K issue has increased, so has the level of debate about Y2K myths and realities. Where possible, the Council has been working to separate fact from fiction -- in our quarterly assessment reports, at public events and press conferences, in Y2K Community Conversations held across the country, and most recently through our new *Y2K and You* booklet and "Y2K Preparedness Checklist." I appreciate the opportunity today to address some of the myths and realities that I think are most important for the public to understand with less than two months remaining until January 1.

One of the more troubling Y2K myths is the notion that January 1 is a seminal date on which everything, or nothing, Y2K-related will occur. A corollary of this myth is that we will all be able to "close the books" on the Y2K issue and declare victory or defeat by the end of New Year's Day. As you know, Year 2000 challenges can happen any time a computer that is not Y2K-compliant comes into contact with a Year 2000 date – before or after January 1. In fact, a number of businesses and governments have already had to use Year 2000 dates in their

automated operations. Information technology professionals are well aware that the Y2K challenge is not limited to January 1 and will be monitoring systems well into the New Year for flaws in billing and financial cycles and possible slow degradations in service. So I think it is important for the public to know that January 1 is just one of the important dates in the life of the Y2K issue.

Another important myth deals with the reporting of Y2K readiness data. It goes something like this: Self-reported Y2K information is not valid since people will not voluntarily report problems, so virtually everything we've heard in terms of industry and government progress reports cannot be believed. This is not true for several reasons. Most organizations have structures in place whereby independent authorities have been reviewing the results of Y2K testing. In some industries, such as electric power, government agencies have conducted selected audits of the reported information and found no major discrepancies. And, most importantly, the industry surveys done for the President's Council have been conducted pursuant to the "Year 2000 Information and Readiness Disclosure Act," which the Congress passed at our urging last year. This Act guarantees individual companies that their responses to these surveys will be treated confidentially, which substantially increases the likelihood of candid responses.

We cannot rule out entirely the possibility that someone, somewhere has at one time or another created a rosier report of their Y2K progress than justified to appease their superiors or shareholders, but I think the overwhelming majority of self-reporting has been very responsible. As I've often said, if the self-reporting on Y2K was truly like allowing students to grade their own papers, everyone should have reported total compliance a long time ago. It would have saved countless organizations months, and in some cases years, of bad publicity. Instead, some companies in the surveys we've been provided have noted that they were behind industry goals or the majority of their peers.

Finally, I'd like to address some of the myths that take the form of Y2K "doomsday" scenarios such as the claims that the Y2K issue will cause nuclear weapons to launch themselves, the Federal Government is planning to use the Y2K issue as an excuse to "take control" of key institutions in the United States, and problems related to the date change will cause all foreign trade to grind to a halt. None of the available information suggests that any of these stories are true. Nuclear weapons require human intervention to launch, no computer malfunction -- Y2K or otherwise -- will cause weapons to fire themselves. However, we are concerned about the ability of the Russian early warning systems to function effectively during the rollover period. We are pleased that Russia has agreed to participate with us in a joint stability center in Colorado, where we will share information from our early warning system to ensure that there are no misunderstandings.

I would also like to stress that the Federal Government is not planning to use the date change as an excuse to usurp the authority of existing organizations. To the contrary, the Y2K challenge's complex nature and vast scope has caused the Federal Government to advise State and local governments that they need to be prepared to respond to possible Y2K problems on their own, at least initially. With regard to foreign trade, the developed countries most important to U.S trade, such as Mexico and Canada, appear to be in good shape for the date change and

vital areas such as international shipping and air transport are reporting increasing levels of compliance. While some developing countries are likely to experience some Y2K failures, which could create difficulties for those who are trading with companies in these countries, there is no indication that these problems will have a negative impact on the overall U.S. economy.

There are a number of Y2K realities, as well as myths, that deserve our attention as well. I'd like to address two such realities. First, it is important for the public to know that our basic national infrastructure is ready for the date change. The information provided to the President's Council and the public indicates that the electric power grids, telecommunications networks, financial transaction systems, and key national transportation systems will make a successful transition to the Year 2000. According to the most recent industry and government assessments, 99 percent of the nation's electricity supply is ready, 99.6 percent of banks are ready, all of the local and long distance carriers that serve over 90 percent of the American public are ready, and the air traffic control system as well as most airports and major airlines are ready.

The second Y2K reality is that, in spite of all of our best efforts to fix and test systems, there will be problems. Not every system will be fixed before January 1, and no amount of testing can ensure perfection. We have already seen Y2K problems surface in instances where systems had been fixed and tested, as was the case for some of the minor problems that a few Federal agencies experienced with the transition to fiscal year 2000. We also expect failures in sectors where large numbers of organizations were late in starting or, even more troubling, are taking a "wait-and-see approach." The important thing is for all organizations to be monitoring their systems for Y2K problems during the rollover period and to have updated contingency plans to allow them to minimize any disruptions that could be created.

Federal Government Rollover Activities – Information Coordination Center

The subcommittees have heard in recent testimony from the Office of Management and Budget about the progress of Federal agency remediation efforts, as well as contingency and "Day One" planning. I will therefore provide a brief overview of the activities of the Council's Information Coordination Center (ICC). The ICC will be the Federal Government's central point for coordinating a wide range of information on system operations and events related to the Y2K transition that will be collected by government emergency centers and the private sector. The ICC will gather information about system operations in Federal agencies; among State, local, and tribal governments; in critical areas of the private sector; and internationally.

To accomplish this task, we are relying to the greatest extent possible on existing structures and expertise. Domestically, information on system operations will be collected by the States and provided through normal channels to FEMA, which will review the reports and pass them on to the ICC. In addition, the ICC will receive reports from national information centers established, many for the first time, by the private sector. The status reports will be provided to appropriate lead agencies. In the case of electric power, for example, the Department of Energy will receive the industry reports, analyze them, and forward the information to the ICC. In addition to electric power, we presently have agreements with the

banking, finance, telecommunications, oil, gas, airline, pharmaceutical and retail industries to operate information centers during the rollover period and to share information with the ICC.

The ICC will receive international status reports from the State Department, the Defense Department, the intelligence agencies, private sector information centers and national Y2K coordinators around the world. In addition, the ICC will work with the National Infrastructure Protection Center and Computer Emergency Response teams here and around the world to monitor unauthorized intrusions into systems.

Information gathered by the ICC will be the basis for complete, regularly updated national and international status reports that will be provided to all Federal agencies and organizations sharing information with the center. These reports will help agency decision-makers determine what, if any, Federal actions are appropriate in response to Y2K-related difficulties. Status reports will also be provided on a regular basis to the public.

The ICC has been testing data collection methods with agency operations centers and private sector information partners. We also conducted a limited training exercise in gathering information from Federal agencies related to the so-called 9/9/99 problem. More extensive training sessions are planned for November and December. The ICC will begin 24-hour monitoring operations on December 28, 1999, continuing through the first few days of January 2000 or longer if conditions warrant.

Personal Preparedness

As I mentioned earlier, based on the available information, we do not believe the Y2K issue will create significant problems in the United States, but no one can rule out the possibility that there won't be temporary disruptions in some services. We believe it is likely that any disruptions will be short-lived, like temporary problems caused by storms, and will not cause long-term challenges. In light of that situation, the Council is advising the public to take reasonable steps to prepare themselves and their families for the date change.

At the beginning of this month, we published *Y2K and You*, an informational booklet on the Y2K issue as well as a "Y2K Preparedness Checklist," which I am submitting as part of the record. The checklist is an expansion of the Council's previous guidance on personal readiness for the Year 2000. Our suggestions include preparing for the long holiday weekend by having at least a three-day supply of food and water, keeping copies of important records before and after January 1, 2000, and checking with manufacturers to make sure that home electronic equipment is Y2K ready.

It is important to note, however, that we are advising individuals to adapt the recommendations in the checklist to their own personal situations and Y2K information made available by their local service providers. I think the most important Y2K information any of us can have is about the readiness of our own communities. There is no "one size fits all" for the entire country with regard to preparing for Y2K. People need to take the time to read Y2K notices being provided by local governments, banks, phone and power companies, supermarkets,

and others so that they have a better understanding of what to expect in their neighborhoods and can prepare accordingly.

Perhaps most importantly, whatever people are going to do to prepare, they should do it early. If everyone waits until the last moment to take even modest precautions, supply systems could be overwhelmed.

Conclusion

When I appeared before you in January of this year, I closed by saying that overreaction by the public to real or perceived Y2K risks was in some ways our greatest challenge. I still believe that. On the other hand, our goal is not public complacency. All of us need to encourage the public to take the appropriate steps to be ready for date change. As I said in January, the way to achieve this delicate balance is to provide people with as much information as possible about Y2K readiness efforts – the good and the bad. Thank you for the opportunity to discuss these important issues with you today.

I would be pleased to answer any questions you may have at this time.

JOHN A. KOSKINEN

Deputy Director for Management
Office of Management and Budget

John A. Koskinen has been Deputy Director for Management at OMB since 1994, a position to which he was nominated by President Bill Clinton, and was confirmed by the U.S. Senate. He is responsible for OMB oversight of Federal regulations, Federal information and computer policies, Federal procurement policies, Federal financial management policies, and management and program evaluation practices in Federal agencies. Prior to returning to public service, Mr. Koskinen was President of The Palmieri Company, a which restructured a range of large, troubled operating companies.

During Mr. Koskinen's 21 years with The Palmieri Company, he helped reorganize the Penn Central Transportation Company; Levitt and Sons, Incorporated; Baldwin-United Corporation, a large diversified financial services company; and Mutual Benefit Life Insurance Company, the largest failed life insurance company in U.S. history.

Prior to joining The Palmieri Company, Mr. Koskinen served as law clerk to Judge David L. Bazelon, Chief Judge, United States Court of Appeals, Washington, D.C.; was associated with Gibson, Dunn & Crutcher in Los Angeles as an attorney; was Special Assistant to the Deputy Executive Director of the National Advisory Commission on Civil Disorders; represented Mayor John Lindsay and New York City in Washington; and served for four years as administrative assistant to Senator Abraham A. Ribicoff of Connecticut.

Mr. Koskinen was born in Cleveland, Ohio, on June 30, 1939; attended high school in Ashland, Kentucky; graduated Magna Cum Laude from Duke University in 1961, where he was a member of Phi Beta Kappa; graduated with an LL.B., cum laude, from Yale Law School in 1964; and did post graduate work in international law at Cambridge University, Cambridge, England, 1964-65.

Mr. Koskinen presently serves as Chairman of the Board of Trustees of Duke University and is a past President of the University's National Alumni Association. He was a Trustee for 12 years of the Cooperative Assistance Fund and also served for 12 years as an organizer and director of the National Captioning Institute. He also served as Chairman of the Washington, DC Host Committee for the 1994 World Cup and is Chairman of the Washington 1996 Olympic Soccer Committee.

Mr. Koskinen and his wife, the former Patricia Salz, and their two children, Cheryl and Jeffrey, live in Washington, D.C.

Chairwoman MORELLA. Thank you, Mr. Koskinen.

I am now pleased to recognize Mr. Willemssen. But as I do, I just want to comment on the fact that the GAO mission is to independently audit all Federal Government agencies and we have worked very closely with GAO over the past 3½ years on the year 2000 computer problem. Just as John Koskinen has demonstrated an exemplary dedication and commitment to public service, so has Joel Willemssen. He has always been ready to assist. His contributions to our House Y2K Working Group's efforts cannot be understated. He has been very much appreciated. And while he may have been a thorn in the side of agencies that required greater congressional attention, he is also one of the reasons that those agencies have redoubled their efforts to comply with the Y2K computer glitch. So, in welcoming Mr. Koskinen, I welcome Mr. Willemssen for his comments.

TESTIMONY OF JOEL C. WILLEMSSEN

Mr. WILLEMSSEN. Thank you very much, Chairwoman Morella. Thank you for inviting us to testify today. And as requested, I will briefly summarize our statement.

In early 1997, we identified Y2K as a high risk area for the Federal Government. Since that time, we have observed substantial progress in the Federal Government's Y2K readiness. While this progress has been significant, it has not been uniform among all Federal agencies. Some agencies have long had strong Y2K programs, others have made dramatic improvements, while still others must continue to be monitored carefully.

For example, on one end of the spectrum is the Social Security Administration, which started its program 10 years ago, has been very responsive to any issues that have surfaced, and has been a government-wide leader in such areas as contingency planning and day one planning. Departments such as Veterans Affairs and Education have made major strides in readiness after relatively slow starts. Other agencies and departments have also made major progress, but still need to be monitored closely because of the criticality of information systems to their missions and the work that remains outstanding. These agencies would include: the Health Care Financing Administration, the Department of Defense, FAA, and IRS. For example, DOD reports that it still has 31 mission critical systems that are not Y2K compliant, 6 of these are not expected to be compliant until December.

Beyond the compliance of individual systems, significant progress has also been made in improving the Government's overall approach. For example, OMB has identified 43 high impact programs as the Government's top priorities. Further, agencies are performing end-to-end testing of multiple systems supporting key business functions, and they have developed business continuity and contingency plans and day one strategies.

Regarding State governments, the available information indicates that States have greatly improved their readiness during this year, with only 4 States now reporting less than 75 percent of mission critical systems completed compared to 40 States reporting this status earlier this year. Nevertheless, there is still much work to do for many of these States. For example, as we testified last

month, many States were not planning to be compliant for some key human services programs, such as Medicaid, Food Stamps, and Child Support Enforcement, until last quarter of 1999.

Y2K is also a challenge for the public infrastructure and key economic sectors. Our work has identified sectors that are clearly leaders on Y2K, while others are lagging behind. For example, banking and finance have clearly been a Y2K leader. Among the areas most at risk, however, are health care and education.

For health care, we have testified on numerous occasions on the risks facing Medicare, Medicaid, and biomedical equipment. We remain concerned about the overall readiness of this sector.

Regarding education, recent surveys conducted by the Federal Department of Education show that many school districts and postsecondary institutions are not yet compliant. In September, our report on the Y2K readiness of 25 of the Nation's largest school districts revealed that only 7 believed that all their mission critical systems were compliant, and 9 said they didn't plan to finish until December.

That concludes a summary of my statement. I will be pleased to address any questions you may have. Thank you.

[The prepared statement of Mr. Willemssen follows:]

United States General Accounting Office

GAO Testimony

Before the Subcommittee on Technology, Committee on Science, and the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives

YEAR 2000 COMPUTING CHALLENGE

For Release on Delivery
Expected at
2:00 p.m. EST
Thursday,
November 4, 1999

Noteworthy Improvements in Readiness But Vulnerabilities Remain

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

GAO/T-AIMD-00-37

Ms. Chairwoman, Mr. Chairman, and Members of the Subcommittees:

Thank you for inviting us to participate in today's hearing on the Year 2000 problem. According to the report of the President's Commission on Critical Infrastructure Protection, the United States—with close to half of all computer capacity and 60 percent of Internet assets—is the world's most advanced and most dependent user of information technology.[1] Moreover, America's infrastructures are a complex array of public and private enterprises with many interdependencies at all levels. These many interdependencies among governments and within key economic sectors could cause a single failure to have adverse repercussions in other sectors.

Because of its urgent nature and the potentially devastating impact it could have on critical government operations, in February 1997 we designated the Year 2000 problem a high-risk area for the federal government.[2] Since that time, we have issued over 150 reports and testimony statements detailing specific findings and numerous recommendations related to the Year 2000 readiness of a wide range of federal agencies.[3] We have also issued guidance to help organizations successfully address the issue.[4]

The public faces the risk that critical services provided by the government and the private sector could be disrupted by the Year 2000 computing problem. As we have previously testified, financial transactions could be delayed, flights grounded, power lost, and national defense affected.[5] Substantial progress has been made to reduce these risks and, in the fast-paced environment of the Year 2000 issue, progress continues to be made.

---

[1]*Critical Foundations: Protecting America's Infrastructures* (President's Commission on Critical Infrastructure Protection, October 1997).
[2]*High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1997).
[3]A list of these publications is included as an attachment to this statement. These publications can be obtained through GAO's World Wide Web page at *www.gao.gov/y2kr.htm*.
[4]*Year 2000 Computing Crisis: An Assessment Guide* (GAO/AIMD-10.1.14, issued as an exposure draft in February 1997 and in final form in September 1997); *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD-10.1.19, issued as an exposure draft in March 1998 and in final form in August 1998); *Year 2000 Computing Crisis: A Testing Guide* (GAO/AIMD-10.1.21, issued as an exposure draft in June 1998 and in final form in November 1998); and *Y2K Computing Challenge: Day One Planning and Operations Guide* (GAO/AIMD-10.1.22, issued as a discussion draft in September 1999 and in final form in October 1999).
[5]*Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Mitigate Risk of Major Disruptions* (GAO/T-AIMD-98-262, August 13, 1998).

Today, I will discuss the federal government's progress and challenges that remain in correcting its systems; identify state and local government Year 2000 issues; and provide an overview of available information on the readiness of key public infrastructure and economic sectors.

FEDERAL GOVERNMENT'S PROGRESS NOTEWORTHY BUT ADDITIONAL WORK REMAINS

As the Year 2000 has grown nearer, the federal government's response to the problem has increased. Mr. Chairman, when we first testified on this problem before you in February 1997, we stated that there was much that needed to be done if the federal government was to avoid the disruption of important services, and that correcting the Year 2000 problem would be labor-intensive and time-consuming.[6] Moreover, we testified that whether agencies succeeded and/or failed would be largely influenced by the quality of executive leadership and program management. As we reported last month, the government's Year 2000 efforts have reinforced an understanding of the importance of consistent and persistent top management attention.[7]

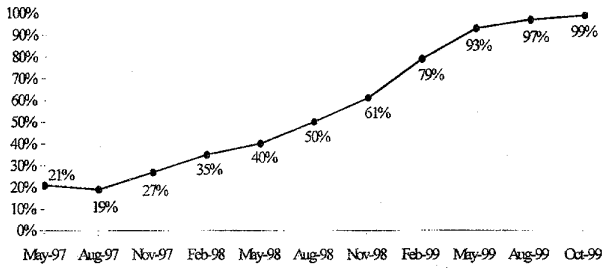
The Year 2000 problem has also demonstrated the importance of congressional and executive branch leadership. At the urging of congressional leaders and others, the Office of Management and Budget (OMB) and the federal agencies have dramatically increased the amount of attention and oversight given to the Year 2000 issue. Moreover, the establishment of the President's Council on Year 2000 Conversion—chaired by an Assistant to the President and consisting of one representative from each of the executive departments and from other federal agencies as may be determined by the Chair—focused attention on the problem and provided a forum for high-level communication among leaders in government, the private sector, and the international community.

The success of these organizations' efforts is demonstrated by chart 1, which shows that

[6] *Year 2000 Computing Crisis: Strong Leadership Today Needed To Prevent Future Disruption of Government Services* (GAO/T-AIMD-97-51, February 24, 1997).
[7] *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-1, October 1, 1999).

the major departments and agencies have progressed from a reported compliance rate of 21 percent in May 1997 to a reported 99 percent in October 1999. While this reported governmentwide progress is notable, the Departments of Defense, Justice, and the Treasury and the U.S. Agency for International Development still have noncompliant systems.

Chart 1: Mission-Critical Systems Reported Year 2000 Compliant, May 1997-October 1999



Source: May 1997 – August 1999 data are from the OMB quarterly reports. The October 1999 data are from OMB's October 29, 1999, testimony before the House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform; and the House Subcommittee on Technology, Committee on Science.

In addition to mission-critical systems, other important areas for agencies are data exchanges, telecommunications, and building systems. Table 1 shows the reported status of the 24 major departments and agencies in these areas as of mid-August. It demonstrates that many agencies have completed work but that several others were not expected to be done until this month or next month.

Table 1: Compliance Status of Data Exchanges, Telecommunications, and Building Systems for the Major Departments and Agencies

Area	Completed	Estimated Date of 1999 Compliance				
		August	September	October	November	December
Data Exchanges[a]	9	2	5	2	2	3
Telecommunications	8	2	9	2	2	1
Building Systems[b]	7	1	7	5	2	1

[a]One agency could not forecast the completion date for its remaining exchanges.
[b]The status was not provided for one agency.

Source: Progress on Year 2000 Conversion: 10th Quarterly Report (OMB, data received August 13, 1999; report issued September 13, 1999).

While governmentwide progress has been significant, such progress has not been uniform among all federal agencies. Some agencies have long had strong Year 2000 programs in place, while others have improved their Year 2000 approaches dramatically although risks remain. Some agencies, however, require continued close attention because of the criticality of information systems to their missions and the work that remains outstanding. The following highlights representative examples of the Year 2000 progress of various agencies.

Social Security Administration (SSA): Since October 1997 we have reported on SSA's governmentwide leadership and significant progress in addressing the Year 2000 problem,[8] although we have identified risk areas (such as the Year 2000 compliance of the systems used by the 54 state Disability Determination Services[9] that help administer the disability programs) and made recommendations to address these risks. In July 1999, we reported that actions to implement these recommendations had either been taken or

[8]*Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain* (GAO/AIMD-98-6, October 22, 1997).
[9]These include the systems in all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

were underway.[10] For example, SSA enhanced its monitoring and oversight of the state Disability Determination Services systems by establishing a full-time project team, designating project managers and coordinators, and requesting biweekly reports.

U.S. Customs Service: In February 1999, we testified that Customs had made good progress in addressing its Year 2000 problem, due in large part to the effective Year 2000 program management structures and processes that it had put into place.[11] Mr. Chairman, in a briefing last month to your Subcommittee staff on the high-impact cross-border inspection service program, we reported that Customs' progress continues. For example, Customs had developed and implemented a Year 2000 master plan and a high-impact area plan, identified and convened external business partners integral to program delivery, and reported that it had completed most planned tasks on or ahead of schedule.

Department of Veterans Affairs (VA): We have been monitoring and evaluating VA's actions to address the Year 2000 problem since 1996. During that time we have made numerous recommendations to reduce the risk associated with Year 2000 failures. VA has been responsive to these recommendations and actions to implement them have either been taken or are underway. For example, in 1998 the Veterans Benefits Administration reassessed its mission-critical efforts for the compensation and pension on-line application and the Beneficiary Identification and Record Locator Sub-System, as well as other technology initiatives to help ensure that these critical undertakings were completed in time. As we testified last week, VA has made much progress in addressing the Year 2000 problem, although some critical tasks remain in areas such as business continuity and contingency planning.[12]

---

[10] *Social Security Administration: Update on Year 2000 and Other Key Information Technology Initiatives* (GAO/T-AIMD-99-259, July 29, 1999).
[11] *Year 2000 Computing Crisis: Customs is Effectively Managing Its Year 2000 Program* (GAO/T-AIMD-99-85, February 24, 1999).
[12] *Year 2000 Computing Challenge: Update on the Readiness of the Department of Veterans Affairs* (GAO/T-AIMD-00-39, October 28, 1999).

Department of Education: In September 1998, we testified that Education was very slow in implementing a comprehensive program to address Year 2000 risks.[13] In particular, significant risks faced the department's student financial aid delivery systems, risks that involved systems testing, exchanging data with internal and external partners, and developing business continuity and contingency plans. More recently, in May 1999 we testified that the Department of Education had made progress toward addressing these risks, although work remained ongoing.[14] We noted that much work on renovating and validating mission-critical systems had been completed and the risk of student financial aid delivery system failures has been significantly reduced. Nevertheless, Education needed to continue making the Year 2000 problem a top priority and focus attention on such issues as end-to-end testing.

Federal Aviation Administration (FAA): In January 1998, we reported FAA had no central Year 2000 program management; an incomplete inventory of mission-critical systems; no overall strategy for renovating, validating, and implementing mission-critical systems; and no milestone dates or schedules.[15] At that time we made several recommendations, including that FAA establish plans to renovate, validate, and test all converted and replaced systems. In September 1999, we testified that FAA had addressed our recommendations and made excellent progress in its Year 2000 readiness.[16] Nevertheless, FAA continued to face challenges in ensuring that its internal systems would work as intended through the year 2000 date change. For example, we found that (1) FAA had not effectively implemented its policy for managing changes to compliant systems, (2) its independent verification efforts were not adequately documented, and (3) its end-to-end testing actions were not comprehensive.

---

[13] *Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems* (GAO/T-AIMD-98-302, September 17, 1998).
[14] *Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains* (GAO/T-AIMD-99-180, May 12, 1999).
[15] *FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically* (GAO/AIMD-98-45, January 30, 1998).
[16] *Year 2000 Computing Challenge: FAA Continues to Make Important Strides, But Vulnerabilities Remain* (GAO/T-AIMD-99-285, September 9, 1999).

Internal Revenue Service (IRS): In February 1999, we testified[17] that IRS had made considerable progress in completing its Year 2000 work since our testimony in May 1998.[18] Nevertheless, it was behind schedule in certain critical tasks, and, in some cases such as the replacement of noncompliant personnel computers, its work is still not complete. Moreover, IRS acknowledges that its review of its information system inventory continues to identify inaccuracies—a significant risk area. Accordingly, IRS reported that, among other activities to improve the quality of its inventory, it has "wall-to-wall" inventory reviews underway at major locations, which are to be completed before the end of the calendar year. In addition, in September we reported that the two IRS business continuity and contingency plans that addressed issuing refunds and receiving paper submissions were inconsistent in two key areas—performance goals and mitigating actions.[19] In testimony before you last week, IRS' Chief Information Officer stated that they had addressed the suggestions in our September report.

Health Care Financing Administration (HCFA): We initially reported on HCFA's Year 2000 program in 1997, making recommendations to improve the agency's program management.[20] In subsequent reports and testimony statements we disclosed that while HCFA had made improvements and had been responsive to our recommendations, critical Year 2000 risks and challenges remained.[21] Most recently, we testified before your Subcommittees in September that HCFA and its contractors had made progress in addressing Medicare Year 2000 issues.[22] However, as stated then, until HCFA had completed its recertification tests that were then ongoing, the final status of the agency's Year 2000 compliance would remain unknown (the tests were due to be completed by

---

[17] *IRS' Year 2000 Efforts: Status and Remaining Challenges* (GAO/T-GGD-99-35, February 24, 1999).
[18] *IRS' Year 2000 Efforts: Status and Risks* (GAO/T-GGD-98-123, May 7, 1998).
[19] *IRS' Year 2000 Efforts: Actions Are Under Way to Help Ensure That Contingency Plans Are Complete and Consistent* (GAO/GGD-99-176, September 14, 1999).
[20] *Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses* (GAO/AIMD-97-78, May 16, 1997).
[21] *Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy* (GAO/AIMD-98-284, September 28, 1998); *Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services* (GAO/T-AIMD-99-92, February 26, 1999); and *Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector* (GAO/T-AIMD-99-160, April 27, 1999).
[22] *Year 2000 Computing Challenge: HCFA Action Needed to Address Remaining Medicare Issues* (GAO/T-AIMD-99-299, September 27, 1999).

November 1, 1999). Moreover, HCFA must also continue to closely monitor contractor testing with providers, which had been limited but which nevertheless had uncovered Year 2000 problems. Accordingly, given the considerable amount of work that remained, we considered it crucial that the development and testing of internal, contractor, and managed care organizations' business continuity and contingency plans move forward rapidly.

Department of Defense (DOD): Our reviews as well as those of the DOD Inspector General indicate that DOD has made noteworthy progress in its Year 2000 activities but that risks remain. For example, in March we testified that DOD had made considerable progress in the prior 3 months[23] but it faced two significant challenges: (1) completing remediation and testing of its mission-critical systems and (2) having a reasonable level of assurance that key processes will continue to work on a day-to-day basis and that key operational missions necessary for national defense can be successfully accomplished. Also, in September 1999 the DOD Inspector General reported that DOD had made significant progress in addressing some risk areas, including identifying and determining the Year 2000 readiness of its critical suppliers. Nevertheless, the Inspector General noted that DOD still faced challenges in ensuring that adequate testing is performed, testing results are sufficiently documented and analyzed, and contingency plans are viable. Moreover, as of November 1, DOD reported that it still had 31 mission-critical systems that were not Year 2000 compliant. Six of these systems are not expected to be compliant until December.

The Government's Approach Has Improved But Risk Areas Remain

While it is important to achieve compliance for individual mission-critical systems, realizing such compliance alone does not ensure that business functions will continue to operate through the change of century—the ultimate goal of Year 2000 efforts. Accordingly, in April 1998 we made recommendations to improve the government's

[23] *Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed* (GAO/T-AIMD-99-101, March 2, 1999).

overall Year 2000 approach.[24] Since that time, the government has made progress in addressing these recommendations, although not all actions are complete.

Priority Setting: Our April 1998 report recommended that governmentwide priorities be set based on such criteria as the potential for adverse health and safety effects, adverse financial effects on American citizens, detrimental effects on national security, and adverse economic consequences. On March 26, OMB implemented our recommendation by issuing a memorandum to federal agencies designating lead agencies for the government's 42 high-impact programs (e.g., food stamps, Medicare, and federal electric power generation and delivery, OMB later added a 43rd high-impact program—the Department of Justice's National Crime Information Center.) For each program, the lead agency was charged with identifying to OMB the partners integral to program delivery; taking a leadership role in convening those partners; assuring that each partner had an adequate Year 2000 plan and, if not, helping each partner without one; and developing a plan to ensure that the program would operate effectively. According to OMB, such a plan might include testing data exchanges across partners, developing complementary business continuity and contingency plans, sharing key information on readiness with other partners and the public, and taking other steps necessary to ensure that the program would work. OMB directed the lead agencies to provide a schedule and milestones of key activities in their plans by April 15, and asked agencies to provide monthly progress reports.

End-To-End Testing: The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, will work as intended in an operational environment. In the case of the year 2000, many systems in the end-to-end chain will have been modified or replaced. As a result, the scope and complexity of testing—and its importance—are dramatically increased, as is the difficulty of isolating, identifying, and correcting problems. Consequently, agencies must work early and continually with their data exchange

[24] *Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships* (GAO/AIMD-98-85, April 30, 1998).

partners to plan and execute effective end-to-end tests. Our Year 2000 testing guide sets forth a structured approach to testing, including end-to-end testing.[25]

Our April 1998 report recommended that, for selected government priorities, lead agencies be designated to ensure that end-to-end testing of these processes and supporting systems occurred across organizational boundaries. On March 31, OMB and the Chair of the President's Council on Year 2000 Conversion announced that one of the key priorities that federal agencies would be pursuing during the rest of 1999 would be cooperative end-to-end testing to demonstrate the Year 2000 readiness of federal programs with states and other partners.

Agencies have also acted to address end-to-end testing. For example, on October 18, we reported that DOD was conducting thousands of end-to-end tests in four major business functions: Health Affairs, Communications, Personnel, and Logistics.[26] Each of the individual test events we attended and reviewed within the four functional areas generally satisfied the key processes that our test guide defines as necessary to effectively plan, conduct, and report on end-to-end testing. We also reported in October that the Department of the Treasury's Financial Management Service, which serves as the government's financial manager, had established effective management controls in performing its portion of Year 2000 end-to-end tests for three critical business functions (Social Security payments, Supplemental Security Income payments, and Internal Revenue Service tax refund payments).[27]

Business Continuity and Contingency Plans: Business continuity and contingency plans are essential. Without such plans, when failures occur, agencies will not have well-defined responses and may not have enough time to develop and test alternatives. Federal agencies depend on data provided by their business partners as well as on

[25]GAO/AIMD-10.1.21, November 1998.
[26]*Defense Computers: DOD Y2K Functional End-to-End Testing Progress and Test Event Management* (GAO/AIMD-00-12, October 18, 1999).
[27]*Year 2000 Computing Challenge: Financial Management Service Has Established Effective Year 2000 Testing Controls* (GAO/AIMD-00-24, October 29, 1999).

services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. Given these interdependencies, it is imperative that contingency plans be developed for all critical core business processes and supporting systems, regardless of whether these systems are owned by the agency. Accordingly, our April 1998 report recommended that agencies be required to develop contingency plans for all critical core business processes.

Since 1998, the federal government has improved its approach to business continuity and contingency planning. OMB has clarified its contingency plan instructions and, along with the Chief Information Officers Council, has adopted our business continuity and contingency planning guide for federal use. In addition, on January 26, 1999, OMB called on federal agencies to identify and report on the high-level core business functions that are to be addressed in their business continuity and contingency plans, as well as to provide key milestones for development and testing of such plans in their February 1999 quarterly reports. In addition, on May 13, OMB required agencies to submit high-level versions of these plans by June 15. In its September 1999 quarterly report, OMB required agencies to submit updated high-level business continuity and contingency plans by October 15, 1999.

As we testified before your Subcommittees last week, although more work remains, agency business continuity and contingency planning has evolved and improved since 1998.[28] In March 1998 we testified that several agencies reported that they planned to develop contingency plans only if they fell behind schedule in completing their Year 2000 fixes.[29] In June 1998, we testified that only four agencies had reported that they had drafted contingency plans for their core business functions.[30] By contrast, in January 1999 we testified that many agencies had reported that they had completed or were

[28] *Year 2000 Computing Challenge: Federal Business Continuity and Contingency Plans and Day One Strategies* (GAO/T-AIMD-00-40, October 29, 1999).
[29] *Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions* (GAO/T-AIMD-98-101, March 18, 1998).
[30] *Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress* (GAO/T-AIMD-98-205, June 10, 1998).

drafting business continuity and contingency plans while others were in the early stages of such planning.[31] Also, as we testified in August, according to an OMB official, all of the major departments and agencies had submitted high-level business continuity and contingency plans in response to OMB's May 13, 1999, memorandum.[32] In October, all of the major departments and agencies and the Postal Service submitted updated high-level plans to OMB.

While OMB's May 1999 memorandum directed agencies to describe their overall strategies and processes for ensuring the readiness of key programs and functions across the agency, it did not detail the format or reporting elements that agencies were to follow. Accordingly, the plans vary considerably in terms of format and level of detail. Some agencies, such as the Departments of Justice and Labor, described their general approach or strategy, while others, such as the Departments of Education and Transportation, provided program or component-entity specific plans that contained more detailed information. With respect to specific elements, all of the plans in our review[33] identified core business processes, as called for in our guide. In addition, we were able to identify 20 agencies that discussed their business continuity and contingency plan validation strategies in their high-level plans. These strategies encompassed a range of activities, including reviews, desktop exercises, simulations, and/or quality assurance audits.

As noted in our business continuity and contingency planning guide, a key element of such a plan is the development of a zero day or Day One risk reduction strategy. In testimony in January 1999, we noted that the Social Security Administration had developed a Day One strategy and suggested that OMB consider requiring other agencies to develop such plans.[34] In its September 1999 quarterly report, OMB subsequently required agencies to submit Day One strategies to it, which each of the 24 major

---

[31]GAO/T-AIMD-99-50, January 20, 1999.
[32]*Year 2000 Computing Challenge: Important Progress Made, Yet Much Work Remains to Ensure Delivery of Critical Services* (GAO/T-AIMD-99-266, August 13. 1999).
[33]While the Department of the Treasury and the General Services Administration reported that they had provided their plans to OMB, we did not receive them in time to include them in our analysis; therefore, we analyzed 23 submissions.
[34]GAO/T-AIMD-99-50, January 20, 1999.

departments and agencies and the Postal Service did. OMB subsequently asked agencies to address seven elements in their plans: (1) a schedule of activities, (2) personnel on call or on duty, (3) contractor availability, (4) communications with the workforce, (5) facilities and services to support the workforce, (6) security, and (7) communications with the public. OMB also told the agencies to consider our Day One strategy guidance carefully.

Our review of agency strategies found that about 40 percent addressed all seven elements.[35] For example, our testimony last week noted that the Department of Veterans Affairs addressed all of OMB's elements.[36] VA and its agencies had developed a Day One strategy that should help the department manage risks associated with the rollover period and better position itself to address any disruptions that may occur. The strategy included a time line of events between December 31 and January 1 and a personnel strategy and leave policy that identifies key managerial and technical personnel available to support Day One operations.

With respect to specific elements, we were able to identify 15 agencies that included a schedule of activities and 17 that addressed staffing issues. In a few cases, agencies addressed either OMB's internal communications element or external communications element but not both. Further, some elements were addressed in a general manner and/or indicated that more work needed to be completed. For example, one agency reported that it is developing procedures to ensure its ability to identify, report, and respond effectively to Year 2000-related events.

[35]While the U.S. Agency for International Development and the General Services Administration reported that they had provided their plans to OMB, we did not receive them in time to include them in our analysis. Therefore, we analyzed 23 agencies' submissions.
[36]GAO/T-AIMD-00-39, October 28, 1999.

STATE AND LOCAL GOVERNMENTS
FACE SIGNIFICANT YEAR 2000 RISKS

Just as the federal government faces significant Year 2000 risks, so too do state and local governments. If the Year 2000 problem is not properly addressed, for example, (1) food stamps and other types of payments may not be made or could be made for incorrect amounts; (2) date-dependent signal timing patterns could be incorrectly implemented at highway intersections, with safety severely compromised; and (3) prisoner release or parole eligibility determinations might be adversely affected.

With respect to state Year 2000 efforts, recent information from the National Association of State Information Resource Executives indicates that states have greatly improved their readiness since the beginning of this year. Table 2 provides a comparison of the percentage of mission-critical systems[37] reported as implemented by the states in January 1999 and in October 1999, which shows that, in general, noteworthy progress has been made during the year.[38]

[37]Mission-critical systems were defined as those that a state had identified as priorities for prompt remediation.
[38]Individual states submit periodic updates to the National Association of State Information Resource Executives. For the October 28 report, about 60 percent of the states submitted their data in October; the oldest data were provided on March 11 and the most recent on October 27.

Table 2: Comparison of Percentages of Mission-Critical Systems Reported as Implemented by the States[a]

Percentage Implemented	Number of States on January 15, 1999[b]	Number of States on October 28, 1999[c]
1-24 percent	9	0
25-49 percent	12	1
50-74 percent	19	3
75-99 percent	6	39
100 percent	0	5

[a]In some cases, states did not report on their mission-critical systems, instead reporting on, for example, processes or on all systems.
[b]Four states did not respond to this question.
[c]Two states did not respond to the survey.

Source: National Association of State Information Resource Executives

In addition to reporting system remediation information, as of October 28, all of the states responding to the National Association of State Information Resource Executives survey reported that they were actively engaged in internal and external contingency planning and that they had established target dates for the completion of these plans. For 9 states, however, the deadline was December 1999.

It is also essential that local government systems be ready for the change of century since critical functions involving, for example, public safety and traffic management, are performed at the local level. Reports on local governments have highlighted Year 2000 concerns. For example:

- In July, we issued a letter on the reported Year 2000 status of the 21 largest U.S. cities.[39] On average, cities reported completing work for 45 percent of the key service areas in which they have responsibility. In addition, 2 cities reported that they had completed their Year 2000 efforts, 9 expected to complete Year 2000 preparations by September 30, 1999, and the remaining 10 cities expected to

[39]*Reported Y2K Status of the 21 Largest U.S. Cities* (GAO/AIMD-99-246R, July 15, 1999).

complete their preparation by December 31.[40] In addition, 7 cities reported completing Year 2000 contingency plans, while 14 reported that their plans were still being developed.

- Also in July, the National League of Cities reported on its survey of 403 cities conducted in April 1999. This survey found that (1) 92 percent of cities had a citywide Year 2000 plan, (2) 74 percent had completed their assessment of critical systems, and (3) 66 percent had prepared contingency plans. (Of those that had not completed such plans, about half stated that they were planning to develop one.) In addition, 92 percent of the cities reported that they expected that all of their critical systems would be compliant by January 1, 2000; 5 percent expected to have completed between 91 and 99 percent, and 3 percent expected to have completed between 81 and 90 percent of their critical systems by January 1.

- In June, the National Association of Counties announced the results of its April survey of 500 randomly selected counties. This survey found that (1) 74 percent of respondents had a countywide plan to address Year 2000 issues, (2) 51 percent had completed system assessments, and (3) 27 percent had completed systems testing. In addition, 190 counties had prepared contingency plans while 289 had not. Further, of the 114 counties reporting that they planned to develop Year 2000 contingency plans, 22 planned to develop the plan in April-June, 64 in July-September, 18 in October-December, and 10 did not yet know.

Of critical importance to the nation are services, such as law enforcement, that are essential to the safety and well-being of individuals across the country. For the most part, responsibility for ensuring the continuity of law enforcement operations resides with thousands of state and local jurisdictions. One critical system—the National Crime Information Center 2000—is operated by the Federal Bureau of Investigation and

[40]In most cities, the majority of city services were scheduled to be completed before this completion date. For example, Los Angeles planned to have all key city systems ready by September 30, except for its wastewater treatment systems, which were expected to be completed in November.

provides law-enforcement users in 80,000 U.S. and foreign agencies critical access to information on criminal activities. Mr. Chairman, we recently briefed your Subcommittee staff on the status of this system. While the Federal Bureau of Investigation reported that its Year 2000 remediation, validation, and implementation activities were completed for the National Crime Information Center 2000, the readiness of five state-level partners was uncertain. Specifically, in assessing the readiness of each state, Puerto Rico, and the District of Columbia, the Bureau found that 47 were Year 2000 ready, but that five had not completed Year 2000 remediation at the time of the assessment. The Bureau plans to continue reviewing the readiness status of these five.

Recognizing the seriousness of the Year 2000 risks facing state and local governments, the President's Council on Year 2000 Conversion developed initiatives to address the readiness of state and local governments. For example:

- The Council established working groups on state and local governments and tribal governments.

- Council officials participate in monthly, multistate conference calls with state Year 2000 coordinators.

- In July 1998, March 1999, and October 1999 the Council, in partnership with the National Governors' Association, convened Year 2000 summits with state and U.S. territory Year 2000 coordinators.

- On May 24, the Council announced a nationwide campaign to promote "Y2K Community Conversations" to support and encourage efforts of government officials, business leaders, and interested citizens to share information on their progress. To support this initiative, the Council developed and is distributing a toolkit that provides examples of which sectors should be represented at these events and issues that should be addressed.

State-Administered Federal Human Services Programs Are At Risk

Among the critical functions performed by states are the administration of federal human services programs. As we reported in November 1998, many systems that support state-administered federal human services programs were at risk, and much work remained to ensure that services would continue.[41] In February of this year, we testified that while some progress had been achieved, many states' systems were not scheduled to become compliant until the last half of 1999.[42] Accordingly, we concluded that, given these risks, business continuity and contingency planning was even more important in ensuring continuity of program operations and benefits in the event of systems failures.

Subsequent to our November 1998 report, OMB directed federal oversight agencies to include the status of selected state human services systems in their quarterly reports. Specifically, in January 1999, OMB requested that agencies describe actions to help ensure that federally supported, state-run programs will be able to provide services and benefits. OMB further asked that agencies report the date when each state's systems will be Year 2000-compliant.

Table 3 summarizes the latest information on state-administered federal human services programs reported by OMB on September 13, 1999.[43] The table indicates that while many states[44] reported their programs to be compliant, a number did not plan to complete Year 2000 efforts until the last quarter of 1999. For example, nine states did not expect to be compliant until the last quarter of 1999 for Child Support Enforcement, seven states for Food Stamps, and four states for Unemployment Insurance. Moreover, Year 2000

[41] *Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs* (GAO/AIMD-99-28, November 6, 1998).
[42] *Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs* (GAO/T-AIMD-99-91, February 24, 1999).
[43] For Medicaid, OMB reports on the two primary systems that states use to administer the program: (1) the Integrated Eligibility System, used to determine whether an individual applying for Medicaid meets the eligibility criteria for participation; and (2) the Medicaid management information system (MMIS), used to process claims and deliver payments for services rendered. Integrated eligibility systems are also often used to determine eligibility for other public assistance programs, such as Food Stamps.
[44] In the context of this testimony, the term states can include the District of Columbia and U.S. territories such as Puerto Rico.

readiness information was unknown in many cases. For example, according to OMB, the status of 16 states' Low Income Home Energy Assistance programs was unknown because applicable readiness information was not available.

Table 2: Reported State-level Readiness for Federally Supported Programs[a]

Program	Compliant[b]	Est. Compliance Date before August 1999[c]	Expected Date of 1999 Compliance					Unk.[d]	N/A[e]
			Aug.	Sept.	Oct.	Nov.	Dec.		
Child Nutrition	41	1	4	4	2	0	2	0	0
Food Stamps	39	0	3	5	3	4	0	0	0
Women, Infants, and Children	45	0	0	2	3	3	1	0	0
Child Care	25	12	0	2	2	3	0	6	4
Child Support Enforcement	23	9	2	7	4	3	2	4	0
Child Welfare	23	14	1	3	5	3	0	5	0
Low Income Home Energy Assistance Program	25	2	3	3	2	0	0	16	3
Medicaid – Integrated Eligibility System	25	18	0	5	4	0	0	2	0
Medicaid – Management Information System	22	16	5	4	4	1	0	2	0
Temporary Assistance for Needy Families	27	15	2	4	2	1	0	3	0
Unemployment Insurance	39	0	0	10	3	0	1	0	1

[a]This chart contains readiness information from the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.
[b]OMB defined compliant as when the state or territory had determined that its systems were able to provide services, whether directly or indirectly, to beneficiaries.
[c]In many cases, the report indicated a date instead of whether the state was compliant. According to OMB, in some cases, while the estimated dates had passed, confirmation of completion had not been received from the federal agencies.
[d]Unk. indicates that, according to OMB, no information was reported by the agency.
[e]N/A indicates that the states or territories reported that the data requested were not applicable to them.

Source: Progress on Year 2000 Conversion: 10th Quarterly Report (OMB, data received August 13, 1999; report issued September 13, 1999).

The information in the OMB report was gathered, but not verified, by the Departments of Agriculture, HHS, and Labor, based on submissions by the states and territories. As a result, some of the state information reported by OMB may not be accurate or up-to-date. For example, in five cases, state programs cited as compliant by OMB in its June quarterly report had estimated compliance dates of October 1999 or later in its September quarterly report.

Further, as we testified last month, the late reported compliance dates of some states are problematic since schedule delays or unexpected problems could well arise.[45] Indeed, reported schedule delays have now occurred in 8 of the 10 state-administered programs since OMB's June 1999 report.[46] For example, OMB's June report showed that three states had estimated compliance dates in the last quarter of 1999 for Food Stamps, while the most recent OMB report indicates that seven states now have estimated fourth quarter compliance dates. To illustrate, the June OMB report indicated that a state and a territory were due to be compliant in June for Food Stamps, but the September OMB report indicated that the date for these entities had moved to November 1999.

In addition to obtaining state-reported readiness information, the three federal departments are taking other actions to assess the ability of state-administered programs to continue operating successfully into the next century.

Department of Agriculture: Agriculture's Food and Nutrition Service (FNS) is responsible for three state-administered federal human services programs—Child Nutrition; Food Stamps; and Women, Infants, and Children. To obtain assurance that state systems are compliant, FNS' regional offices are collecting readiness status information from states as part of their monitoring. Moreover, in June 1999, FNS required its regions to provide, for each program, a copy of either a state letter certifying that it was Year 2000 compliant or a business continuity and contingency plan. As of

[45] *Year 2000 Computing Challenge: Readiness of Key State-Administered Federal Programs* (GAO/T-AIMD-00-9, October 6, 1999).
[46] There was no change in one state-administered federal program, and the number of states with estimated compliance dates in the last quarter declined by one for a second program.

August 25, 1999, FNS had received

- 15 certifications and 6 business continuity and contingency plans for Child Nutrition;
- 22 certifications and 16 business continuity and contingency plans for Food Stamps; and
- 25 certifications and 21 business continuity and contingency plans for Women, Infants, and Children.

Although agency officials instructed FNS regional offices to require state agencies for all three programs to prepare business continuity and contingency plans, it remains unclear whether all states have adequate plans to ensure the continuity of these programs. For example, a June 18 FNS document summarizing the agency's review of contingency plans received to date noted that "all need work. As of September 15, FNS officials told us that only two states had submitted suitable contingency plans. FNS intends to have its contractor review contingency plans for those states that reported that they expected to be compliant after September 30, 1999.

Department of Health and Human Services: Six of the 10 state-administered federal human services programs are overseen by either one of two HHS component entities, HCFA or the Administration for Children and Families (ACF). As we stated in October, HCFA has adopted an approach that includes three rounds of on-site contractor reviews of states (performed in conjunction with HCFA regional and headquarters offices) using a standard methodology.[47] With respect to the risk levels assigned to the states, as of October 4, 1999,

- 4 eligibility systems and 5 MMISs were assessed at high risk,
- 13 eligibility systems and 8 MMISs were assessed at medium risk, and
- 36 eligibility systems and 40 MMISs were assessed at low risk.[48]

[47] *Reported Medicaid Year 2000 Readiness* (GAO/AIMD-00-22R, October 5, 1999).

[48] Forty state risk ratings were based on second-round visits (conducted between May and September 1999), while 13 state risk ratings in the low category are based on the results of first-round visits because the states were not visited in the second round.

HCFA's current state risk ratings represent an overall improvement from those assigned after the first round of reviews, although many issues continue to be unresolved at the states.

To complement its system reviews, HCFA obtained another contractor to review state business continuity and contingency plans. In June 1999, HCFA's business continuity and contingency plan contractor began reviewing the quality of state plans through either a desk audit alone or both a desk audit and an on-site visit. Of the 33 states and two territories that have been reviewed by the contractor as of October 1, 1999,[49] 11 were high risk, 11 were medium risk, and 13 were low risk.

Regarding the other five HHS state-administered federal programs, ACF modeled its state assessment program after that of HCFA. Table 4 shows the number of states placed in each risk assessment level as of October 21.

Table 4: Summary of Risk Levels as of October 21, 1999

Program	Number of State Reports	Risk Levels		
		High	Medium	Low
ACF - Child Care	55	3	16	36
ACF - Child Support Enforcement[a]	54	3	12	39
ACF - Child Welfare[a]	54	0	14	40
ACF - Low Income Home Energy Assistance Program[a]	54	1	16	37
ACF - Temporary Assistance for Needy Families[a]	54	3	9	42

[a]These programs were not evaluated for one of the U.S. territories or a territory does not have the program.

According to an ACF official, although the agency has not completed a reassessment of state risk ratings, most state programs with high or medium risk ratings have improved

[49]As of October 1, 1999, 16 state business continuity and contingency plans had not been reviewed, and 2 states had not provided their plans to HCFA.

their status since the original assessment was completed (May through September).

Department of Labor: With respect to Unemployment Insurance, the 53 State Employment Security Agencies (SESAs) use their own systems to pay unemployment insurance compensation benefits to eligible workers and collect state unemployment taxes from employers. As of November 1, according to the Labor Department, 51 of 53 SESAs reported that their benefits systems were Year 2000 compliant, while 50 of the 53 tax systems were reported as such.

In September 1998, Labor established a valuable tool in gauging the readiness of state Unemployment Insurance systems by requiring that all SESAs arrange for independent verification and validation. Based on the results of these reviews, Labor has indicated that the Secretary will be sending letters to the Governors of 11 states considered to be in need of further attention concerning their Year 2000 compliance efforts. Labor reported to us that it would continue to work aggressively with the SESAs needing further attention.

To provide further assurance that unemployment insurance benefits will continue without interruption in the Year 2000, Labor has required that the SESAs develop detailed business continuity and contingency plans for their automated systems. According to Labor, a PC-based Automated Contingency System has been developed to permit the interim payment of benefits should a Year 2000 failure occur. Labor reports that nine states have adopted this system as part of their contingency planning.

MIXED YEAR 2000 PROGRESS IN KEY SECTORS

Beyond the risks faced by federal, state, and local governments, the year 2000 also poses a serious challenge to the public infrastructure, key economic sectors, and to other countries. To address these concerns, in April 1998 we recommended that the President's Council use a sector-based approach and establish the effective public-private

partnerships necessary to address this issue.[50] The Council subsequently established over 25 sector-based working groups, and has been initiating outreach activities since it became operational last spring. In addition, the Chair of the Council has formed a Senior Advisors Group of representatives from private-sector firms across key economic sectors. Members of this group are expected to offer perspectives on cross-cutting issues, information sharing, and appropriate federal responses to potential Year 2000 failures.

Our April 1998 report also recommended that the President's Council develop a comprehensive picture of the nation's Year 2000 readiness, to include identifying and assessing risks to the nation's key economic sectors--including risks posed by international links. In October 1998 the Chair directed the Council's sector working groups to begin assessing their sectors. The Chair also provided a recommended guide of core questions that the Council asked to be included in surveys by the associations performing the assessments. These questions included the percentage of work that has been completed in the assessment, renovation, validation, and implementation phases. The Council then began issuing quarterly public reports summarizing these assessments, beginning in January 1999.

The Council's August 1999 report stated that important national systems will make a successful transition to the year 2000 but that much work, such as contingency planning, remains to be done.[51] In particular, the Council expressed a high degree of confidence in five major domestic areas: financial institutions, electric power, telecommunications, air travel, and the federal government. For example, the Council stated that on August 2, federal bank, thrift, and credit union regulators reported that 99 percent of federally insured financial institutions have completed testing of critical systems for Year 2000 readiness.

[50]GAO/AIMD-98-85, April 30, 1998.
[51]The Council's three reports are available on its web site, *www.y2k.gov*. The Council's next report is due to be released shortly.

The Council had concerns in four significant areas: local government, health care, education, and small businesses. For example, according to the Council report, many school districts could move into the new century with dysfunctional information technology systems, since only 28 percent and 30 percent, respectively, of Superintendent/Local Educational Agencies and post-secondary institutions reported that their mission-critical systems were Year 2000 compliant.

In the international arena the Council stated that the Year 2000 readiness of other countries was improving but remains a concern. The Council reported that the June 1999 meeting of National Year 2000 Coordinators held at the United Nations found that the 173 countries in attendance were clearly focused on the Year 2000 problem but that many will likely not have enough time or resources to finish preparations before the end of 1999.

In addition to our work related to federal, state, and local government Year 2000 progress, we have also issued several publications related to key economic sectors. Our analysis has identified sectors that are leaders in resolving Year 2000 problems, others that require sustained attention because of their importance and continued risk, and a few that are lagging behind. In addition, variance in the level of readiness within segments of a sector can exist. The following are representative samples of the readiness of key sectors.

Banking and Finance Sector: The banking and finance sector is considered a Year 2000 leader. A large portion of the institutions that make up this sector are overseen by one or more federal regulatory agencies. In September 1998 we testified on the efforts of five federal financial regulatory agencies[52] to ensure that the institutions they oversee are ready to handle the Year 2000 problem.[53] Regulators had made significant progress in assessing the readiness of member institutions and in raising awareness on important

[52]The National Credit Union Administration, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Federal Reserve System, and the Office of the Comptroller of the Currency.
[53]*Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain* (GAO/T-AIMD-98-305, September 17, 1998).

issues, such as contingency planning and testing. Regulator examinations of bank, thrift, and credit union Year 2000 activities found that the vast majority were doing a satisfactory job of addressing the problem. Nevertheless, regulators faced the challenge of ensuring that they were ready to take swift action to address those institutions that falter in the later stages of correction, and to address disruptions caused by international and public infrastructure failures.

In April, we reported that the Federal Reserve System--which is instrumental to our nation's economic well-being since it provides depository institutions and government agencies with services such as processing checks and transferring funds and securities—had effective controls to help ensure that its Year 2000 progress is reported accurately and reliably.[54] It also was effectively managing the renovation and testing of its internal systems and the development and planned testing of contingency plans for continuity of business operations. Nevertheless, the Federal Reserve System still had much to accomplish before it was fully ready for January 1, 2000, such as completing validation and implementation of all of its internal systems and completing its contingency plans.

In addition to the domestic banking and finance sector, large U.S. financial institutions have financial exposures and relationships with international financial institutions and markets that may be at risk if these international organizations are not ready for the date change occurring on January 1, 2000. In April, we reported[55] that foreign financial institutions had reportedly lagged behind their U.S. counterparts in preparing for the Year 2000 date change. Officials from four of the seven large foreign financial institutions we visited said they had scheduled completion of their Year 2000 preparations about 3 to 6 months after their U.S. counterparts, but that they planned to complete their actions by mid-1999 at the latest. Moreover, key international market supporters, such as those that transmit financial messages and provide clearing and settlement services, told us that their systems were ready for the date change and that they had begun testing with the

[54]*Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Converston* (GAO/AIMD-99-78, April 9, 1999).
[55]*Year 2000: Financial Institution and Regulatory Efforts to Address International Risks* (GAO/GGD-99-62, April 27, 1999).

financial organizations that depend on these systems. We further found that seven large U.S. banks and securities firms that we visited were taking actions to address their international risks. Finally, U.S. banking and securities regulators were addressing the international Year 2000 risks of the institutions that they oversee.

With respect to the insurance industry, in March, we concluded that the insurance regulator presence in the Year 2000 area was not as strong as that exhibited by the banking and securities industry.[56] State insurance regulators we contacted were late in raising industry awareness of potential Year 2000 problems, provided little guidance to regulated institutions, and failed to convey clear regulatory expectations to companies about Year 2000 preparations and milestones. Nevertheless, the insurance industry is reported by both its regulators and by other outside observers to be generally on track to being ready for 2000. However, most of these reports are based on self-reported information and, compared with other financial regulators, insurance regulators' efforts to validate this information generally began late and were more limited.

In a related report, in April[57] we stated that variations in oversight approaches by state insurance regulators also made it difficult to ascertain the overall status of the insurance industry's Year 2000 readiness. We reported that the magnitude of insurers' Year 2000-related liability exposures could not be estimated at that time but that costs associated with these exposures could be substantial for some property-casualty insurers, particularly those concentrated in commercial-market sectors. In addition, despite efforts to mitigate potential exposures, the Year 2000-related costs that may be incurred by insurers would remain uncertain until key legal issues and actions on pending legislation were resolved.

Telecommunications: In September, we reported that basic network services are unlikely to be immediately disrupted by Year 2000-related problems if networks are left

[56] *Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness* (GAO/T-GGD-99-56, March 11, 1999).
[57] *Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness* (GAO/GGD-99-87, April 30, 1999).

unremediated, according to experts who have been tracking and studying the telecommunications industry's Year 2000 risks.[58] However, telecommunications carriers could still experience problems with network maintenance, service billing, or operator interfaces, such as incorrect date or day-of-week displays. We also said that major U.S. public telecommunications carriers reported making good progress in remediating their networks and supporting systems in order to prevent these types of Year 2000-related problems. Less information was available on the status of medium and small carriers but efforts to collect more data on these carriers were ongoing.

From an international telecommunications perspective, in July 1999, the Network Reliability and Interoperability Council reported that while countries around the globe continue to make progress, their efforts—with some exceptions—have not matched the pace of efforts in the United States and Canada. Regions considered to be at high risk were Central and South America (including Mexico), the Indian sub-continent, Sub-Sahara Africa, Eastern Europe, the Middle East and North Africa (excluding Israel), and Asia Pacific. The Network Reliability and Interoperability Council cautioned, however, that the information available was limited and varied in its view from source to source. Moreover, the results of the assessment varied widely within each region. For example, while Asia Pacific is considered to be a region of high risk, some nations within that region, such as Australia, are considered to be at low risk.

Energy Sector: As we testified last week, while progress had been made in making the nation's nuclear power plants and fuel processing facilities Year 2000 ready, some risk remained.[59] At particular risk were the two plants that do not yet have their non-safety systems ready, especially the one with a completion date scheduled for more than 30 days from now. Similarly, the four nuclear fuel facilities that were not Year 2000 ready by September 1, 1999, raise concern. Likewise, not knowing the current Year 2000 status of all 14 decommissioned plants with spent fuel also raised concern. Finally, the lack of

[58] *Year 2000 Computing Crisis: Readiness of the Telecommunications Industry* (GAO/AIMD-99-293, September 30, 1999).
[59] *Y2K Computing Challenge: Nuclear Power Industry Reported Nearly Ready; More Risk Reduction Measures Can Be Taken* (GAO/T-AIMD-00-27, October 26, 1999).

information on two key issues—independent reviews of Year 2000 testing and emergency Year 2000 exercises—and the lack of requirements for Day One planning increases the Year 2000 risk to the nuclear power industry.

To further reduce risks, we pointed out that the Nuclear Regulatory Commission (NRC) and the nuclear power industry could still take specific actions to ensure Year 2000-related plant safety.

- First, NRC should evaluate and report on the Year 2000 status of all decommissioned plants with spent fuel status that previously reported that they were not Year 2000 ready.
- Second, NRC should survey the 103 operational nuclear power plants to gain an understanding of what independent reviews were completed. Based on this information, NRC should then identify plants that may need additional reviews.
- Third, NRC should obtain information on the scope and extent of nuclear power plants' emergency exercises, and whether these exercises have incorporated Year 2000 scenarios.
- Finally, NRC should ensure that all nuclear facilities have developed Day One plans.

In April, we reported that while the electric power industry had concluded that it had made substantial progress in making its systems and equipment ready to continue operations into the year 2000, significant risks remained since many reporting organizations did not expect to be Year 2000 ready within the June 1999 industry target date.[60] We therefore suggested that the Department of Energy (1) work with the Electric Power Working Group to ensure that remediation activities were accelerated for the utilities that expected to miss the June 1999 deadline for achieving Year 2000 readiness, and (2) encourage state regulatory utility commissions to require a full public disclosure of Year 2000 readiness status of entities transmitting and distributing electric power.

[60] *Year 2000 Computing Crisis: Readiness of the Electric Power Industry* (GAO/AIMD-99-114, April 6, 1999).

Subsequent to our report, on August 3, 1999, the North American Electric Reliability Council released its fourth status report on electric power systems. This report disclosed those organizations that were Year 2000 ready or Year 2000 ready with limited exceptions. According to the Council, as of June 30, 1999, 251 of 268 (94 percent) of bulk electric organizations were Year 2000 ready or Year 2000 ready with limited exceptions.[61] In addition, this report stated that 96 percent of local distribution systems were reported Year 2000 ready.[62] The North American Electric Reliability Council stated that the information it uses is principally self-reported but that 84 percent of the organizations reported that their Year 2000 programs had also been audited by internal and/or external auditors.

In May we reported[63] that while the domestic oil and gas industries had reported that they had made substantial progress in making their equipment and systems ready to continue operations into the year 2000, risks remained. For example, although over half of our oil is imported, little was known about the Year 2000 readiness of foreign oil suppliers. Further, while individual domestic companies reported that they were developing Year 2000 contingency plans, there were no plans to perform a national-level risk assessment and develop contingency plans to deal with potential shortages or disruptions to the nation's overall oil and gas supplies. We suggested that the Council's oil and gas working group (1) work with industry associations to perform national-level risk assessments and develop and publish credible, national-level scenarios regarding the impact of potential Year 2000 failures, and (2) develop national-level contingency plans.

The results of the latest oil and gas industry survey were provided at the October 21 Federal Energy Regulatory Commission Technical Conference. This survey found that

[61]The North American Electric Reliability Council reported that 64 of these organizations had exceptions but that it "believes that the work schedule provided to complete these exception items in the next few months represents a prudent use of resources and does not increase risks associated with reliable electric service into the Year 2000."

[62]This was based on the percentage of the total megawatts of the systems reported as Year 2000 ready by investor-owned, public power, and cooperative organizations. The report did not identify the number of local distribution organizations that reported that they were Year 2000 ready.

[63]*Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries* (GAO/AIMD-99-162, May 19, 1999).

92 percent of oil and gas companies' business systems, 93 percent of their embedded systems, and 83 percent of their supply chain were Year 2000 ready. In addition, the survey found that 90 percent of the oil and gas companies had contingency plans in place, and 77 percent had tested them.

Transportation Sector: A key component of the nation's transportation sector are airports. In January we reported on our survey of 413 airports, finding that while the nation's airports were making progress in preparing for the year 2000, such progress varied.[64] Of the 334 airports responding to our survey, about one-third reported that they would complete their Year 2000 preparations by June 30, 1999. The other two-thirds either planned on a later date or failed to estimate any completion date. Moreover, about half of the airports in our survey did not have contingency plans for any of 14 core airport functions. Although most of those not expecting to be ready by June 30 were small airports, 26 of them were among the nation's largest 50 airports.

More recently, we testified in September on the Year 2000 information collected by the Federal Aviation Administration on 113 U.S. airports.[65] According to FAA's information at that time, about 20 percent of the 113 airports reported that they had completed their Year 2000 preparations. Another 58 percent estimated that they would complete Year 2000 efforts by September 30, and the remaining 22 percent either planned on a later date or did not provide an estimated completion date. Among the group planning to complete their Year 2000 efforts after September 30 but by November 30 were five of the nation's largest international airports.

Just 2 days ago, the Department of Transportation announced that none of the 565 airports regulated by FAA had been found to have Year 2000 problems that will affect their ability to meet regulatory safety requirements—which would include airfield operations such as aircraft rescue and firefighting response but not ground transportation

[64] *Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem* (GAO/RCED/AIMD-99-57, January 29, 1999).
[65] GAO/T-AIMD-99-285, September 9, 1999.

systems. To make this assessment, FAA determined whether airport operators had taken the necessary measures to ensure that such systems were Year 2000 compliant or had developed an alternate means for complying with these requirements. For example, in the case of runway and taxiway lighting, FAA required that an airport operator ensure that computers used to control these lights were Year 2000 compliant or that control of the lights could be performed manually.

Another essential element in this sector is the readiness of airlines. According to FAA's information at the time of our September testimony, about 33 percent of 146 airlines reported that their systems were Year 2000 compliant. Another 35 percent planned to complete their Year 2000 efforts by September 30, and the remaining 32 percent either planned on a later date or did not provide any date. Among the group planning to complete their Year 2000 work after September 30 but by December 31, 1999 were four of the nation's major airlines.

Education: On September 21, we reported on the Year 2000 readiness status of 25 large school districts, showing that much work remained.[66] Of the 25 school districts surveyed, 7 reported that all of their systems that support mission-critical business functions were Year 2000 compliant. Two districts reported that their mission-critical systems would be Year 2000 compliant by the end of September. The remaining 16 districts reported that their systems would be ready by the last quarter of 1999 or later, including nine reporting that compliance would be achieved after November 30, 1999.

More recently, Education completed surveys of a random sample of 1,200 school districts and 1,600 postsecondary institutions during the first week of October. Regarding the 985 school district respondents, (1) 64 percent reported that all mission-critical systems were compliant, (2) 96 percent expected that all of their mission-critical systems would be compliant by January 1, 2000, (3) 65 percent reported that contingency plans were completed, and (4) 83 percent expected that contingency plans would be completed by

[66] *Reported Year 2000 (Y2K) Readiness Status of 25 Large School Districts* (GAO/AIMD-99-296R, September 21, 1999).

January 1. For the 1,352 postsecondary institutions respondents, (1) 61 percent reported that all mission-critical systems were compliant, (2) 97 percent expected that all of their mission-critical systems would be compliant by January 1, 2000, (3) 73 percent reported that contingency plans were completed, and (4) 88 percent expected that contingency plans would be completed by January 1.

Health Care Sector: This sector, which includes health care providers (such as hospitals and emergency health care services), insurers (such as Medicare and Medicaid), and biomedical equipment, is not as far along in its readiness as other sectors. In July we reported[67] that HCFA had taken aggressive and comprehensive outreach action with regard to its over 1.1 million health care providers that administer services for Medicare-insured patients.[68] Despite these efforts, HCFA data showed that provider participation in its outreach activities had been low. Our July report also found that although many surveys had been completed in 1999 on the Year 2000 readiness of health care providers, none of the 11 surveys we reviewed provided sufficient information with which to assess the Year 2000 status of the health care provider community. Each of the surveys had low response rates, and several did not address critical questions about testing and contingency planning.

To reduce the risk of Year 2000-related failures in the Medicare provider community, our July report suggested, that HCFA consider, for example, using additional outreach methods, such as public service announcements, and set milestones for Medicare contractors for testing with providers. We also made suggestions to the President's Council on Year 2000 Conversion's healthcare sector working group, including a suggestion to consider working with associations to publicize those providers who respond to future surveys in order to increase survey response rates.

[67]*Year 2000 Computer Crisis: Status of Medicare Providers Unknown* (GAO/AIMD-99-243, July 28, 1999).
[68]Examples of such providers are hospitals, laboratories, physicians, and skilled nursing/long-term care facilities.

Of Medicare's 39 million beneficiaries, about 6.9 million are enrolled in 383 managed care organizations. We testified in September that HCFA, with assistance from a contractor, performed a risk assessment of 425 managed care organizations[69] using certification statements and associated qualifications, and other criteria.[70] HCFA's June 1999 risk assessment concluded that 94 managed care organizations were high risk (22 percent), 314 were medium risk (74 percent), and 17 were low risk (4 percent). Also, as of September 2, 1999, HCFA had received business continuity and contingency plans from 310 of the 383 managed care organizations. Its review of these 310 plans concluded that 69 percent needed major improvement, 18 percent needed minor improvement, and 13 percent were reasonable.

With respect to biomedical equipment, on June 10 we testified[71] that, in response to our September 1998 recommendation, [72] HHS, in conjunction with the Department of Veterans Affairs, had established a clearinghouse on biomedical equipment. As we recently testified, as of October 4,1999, 4,288 biomedical equipment manufacturers had submitted data to the clearinghouse.[73] About 61 percent of these manufacturers reported having products that do not employ dates and about 8 percent (342 manufacturers) reported having date-related problems such as an incorrect display of date/time. According to the Food and Drug Administration, a component agency of HHS, the 342 manufacturers reported 1,035 specific products with date-related problems. However, not all compliance information was available on the clearinghouse because the clearinghouse referred the user to 429 manufacturers' web sites. Accordingly, we reviewed the web sites of these manufacturers and testified in October that we found a

[69]Since July 1999, the number of managed care organizations decreased from 425 to 383, because 52 left the Medicare program while 10 new managed care organizations joined.
[70]GAO/T-AIMD-99-299, September 27, 1999.
[71]*Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment* (GAO/T-AIMD-99-209, June 10, 1999).
[72]*Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown* (GAO/AIMD-98-240, September 18, 1998).
[73]*Year 2000 Computing Challenge: Compliance Status Information on Biomedical Equipment* (GAO/T-AIMD-00-26, October 21, 1999).

total of 32,598 products.[74] Of these products, 17,505 were reported as not employing a date, 9,585 were reported as compliant, 4,053 were shown as not compliant, and the compliance status of 1,455 was unknown.

In addition to the establishment of a clearinghouse, our September 1998 report[75] also recommended that HHS and the Department of Veterans Affairs take prudent steps to jointly review manufacturers' test results for critical care/life support biomedical equipment. We were especially concerned that the departments review test results for equipment previously deemed to be noncompliant but now deemed by manufacturers to be compliant, or equipment for which concerns about compliance remained. In May 1999, the Food and Drug Administration, announced that it planned to develop a list of critical care/life support medical devices and the manufacturers of these devices, select a sample of manufacturers for review, and hire a contractor to develop a program to assess manufacturers' activities to identify and correct Year 2000 problems for these medical devices. In addition, if the results of this review indicated a need for further review of manufacturer activities, the contractor would review a portion of the remaining manufacturers not yet reviewed.

The Food and Drug Administration identified 90 types of products that it refers to as computer-controlled, potentially high-risk devices, and identified 803 manufacturing sites that produce equipment sold in the United States. Of these sites, a Food and Drug Administration contractor completed 80 site visits and had prepared 62 assessment reports. We reviewed 25 manufacturer site visit reports that were completed by the examiners and available to us as of September 10, 1999. For 20 of these assessments, the examiners' assessed concern was low. At the 5 remaining manufacturers' sites, the examiner found at least one item of moderate concern, such as test planning and

[74]Because of limitations in many of the manufacturers web sites, our ability to determine the total number of biomedical equipment products reported and their compliance status was impaired. Accordingly, the actual number of products reported by the manufacturers could be significantly higher than the 32,598 products that we counted.
[75]GAO/AIMD-98-240, September 18, 1998.

procedures. According to the survey project manager, the areas identified in the site visit reports as medium risk do not constitute a risk to patient health or safety.

In testimony on October 28,[76] we also reported on the results of a Department of Veterans Affairs survey of 517 companies classified as "pharmaceutical firms," "pharmaceutical, other firms," and "medical-surgical firms." As of August 1, of the 186 "pharmaceutical firms" that responded to the survey, 30 percent reported that they were Year 2000 compliant. Of the 72 "pharmaceutical, other firms" that responded to the survey, 39 percent were compliant. Finally, of the 259 "medical-surgical firms" that responded, 56 percent reported that they were compliant.

International: In addition to the risks associated with the nation's key economic sectors, one of the largest and most uncertain area of risk relates to the global nature of the problem. On October 21, we testified that through its leadership of the President's Council's International Relations Working Group, the State Department has worked to increase awareness of the Year 2000 problem throughout the world, collected and shared information on the problem with other federal agencies and foreign nations, and encouraged the remediation of faulty computer systems.[77] Similarly, we found that the U.S. Agency for International Development had devoted resources to assessing what Year 2000 problems could occur at many of its worldwide missions and on projects that it has funded that are currently underway within the countries where these missions are located. The collective efforts of State and the U.S. Agency for International Development to analyze international Year 2000 readiness have shown that some countries will simply not make their Year 2000 deadlines and, in fact, are likely to suffer disruptions in critical infrastructure-related services such as power, water, and finance.

The impact of Year 2000-induced failures in foreign countries could adversely affect the United States, particularly as it relates to the supply chain. To address the international

[76]GAO/T-AIMD-00-39, October 28,1999.
[77]*Year 2000 Computing Chalienge: State and USAID Need to Strengthen Business Continuity Planning* (GAO/T-AIMD-00-25, October 21, 1999).

supply chain issue, in January 1999 we suggested[78] that the President's Council on Year 2000 Conversion prioritize trade and commerce activities that are critical to the nation's well-being (e.g., oil, food, pharmaceuticals) and, working with the private sector, identify options for obtaining these materials through alternative avenues in the event that Year 2000-induced failures in the other country or in the transportation sector prevent these items from reaching the United States. In commenting on this suggestion, the Chair stated that the Council had (1) worked with federal agencies to identify sectors with the greatest dependence on international trade, (2) held industry roundtable discussions with the pharmaceutical and food supply sectors, and (3) hosted bilateral and trilateral meetings with the Council's counterparts in Canada and Mexico—the United States' largest trading partners.

- - - - -

In summary, while much improvement has been shown, additional work remains at the national, federal, state, and local levels to ensure that major service disruptions do not occur. Specifically, remediation must be completed, end-to-end testing performed, and business continuity and contingency plans and Day One strategies developed and validated. Similar actions remain to be completed by the nation's key sectors. Whether the United States successfully confronts the Year 2000 challenge will largely depend on the success of federal, state, and local governments, as well as the private sector working together to complete these actions. Accordingly, strong leadership and partnerships must be maintained to ensure that the needs of the public are met at the turn of the century.

Ms. Chairwoman, Mr. Chairman, this concludes my statement. I would be pleased to respond to any questions that you or other members of the Subcommittees may have at this time.

Contacts

For information about this testimony, please contact Joel Willemssen at (202) 512-6253 or by e-mail at willemssenj.aimd@gao.gov.

[78]GAO/T-AIMD-99-50, January 20, 1999.

GAO REPORTS AND TESTIMONY ADDRESSING THE YEAR 2000 CRISIS

Overall Year 2000 Issues

Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-144, April 14, 1999)

Year 2000 Computing Crisis: Additional Work Remains to Ensure Delivery of Critical Services (GAO/T-AIMD-99-143, April 13, 1999)

High-Risk Series: An Update (GAO/HR-99-1, January 1999)

Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999)

Year 2000 Computing Challenge: Readiness Improving, But Critical Risks Remain (GAO/T-AIMD-99-49, January 20, 1999)

Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress (GAO/T-AIMD-98-205, June 10, 1998)

Year 2000 Computing Crisis: Potential For Widespread Disruption Calls For Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998)

Year 2000 Computing Crisis: Strong Leadership Needed to Avoid Disruption of Essential Services (GAO/T-AIMD-98-117, March 24, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions (GAO/T-AIMD-98-101, March 18, 1998)

Year 2000 Computing Crisis: Success Depends Upon Strong Management and Structured Approach, (GAO/T-AIMD-97-173, September 25, 1997)

Year 2000 Computing Crisis: Time is Running Out for Federal Agencies to Prepare for the New Millennium (GAO/T-AIMD-97-129, July 10, 1997)

Year 2000 Computing Crisis: Risk of Serious Disruption to Essential Government Functions Calls for Agency Action Now (GAO/T-AIMD-97-52, February 27, 1997)

Year 2000 Computing Crisis: Strong Leadership Today Needed To Prevent Future Disruption of Government Services (GAO/T-AIMD-97-51, February 24, 1997)

High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997)

Banking and Finance

Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999)

Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999)

Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999)

Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999)

Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998)

Year 2000 Computing Crisis: Federal Reserve Is Acting to Ensure Financial Institutions Are Fixing Systems But Challenges Remain (GAO/AIMD-98-248, September 17, 1998)

Securities Pricing: Actions Needed for Conversion to Decimals (GAO/T-GGD-98-121, May 8, 1998)

Year 2000 Computing Crisis: Federal Regulatory Efforts to Ensure Financial Institution Systems Are Year 2000 Compliant (GAO/T-AIMD-98-116, March 24, 1998)

Year 2000 Computing Crisis: Office of Thrift Supervision's Efforts to Ensure Thrift Systems Are Year 2000 Compliant (GAO/T-AIMD-98-102, March 18, 1998)

Post-Hearing Questions on the Federal Deposit Insurance Corporation's Year 2000 (Y2K) Preparedness (AIMD-98-108R, March 18, 1998)

SEC Year 2000 Report: Future Reports Could Provide More Detailed Information (GAO/GGD/AIMD-98-51, March 6, 1998)

Year 2000 Computing Crisis: Federal Deposit Insurance Corporation's Efforts to Ensure Bank Systems Are Year 2000 Compliant (GAO/T-AIMD-98-73, February 10, 1998)

Year 2000 Computing Crisis: Actions Needed to Address Credit Union Systems' Year 2000 Problem (GAO/AIMD-98-48, January 7, 1998)

Year 2000 Computing Crisis: National Credit Union Administration's Efforts to Ensure Credit Union Systems Are Year 2000 Compliant (GAO/T-AIMD-98-20, October 22, 1997)

Telecommunications

Year 2000 Computing Crisis: Readiness of the Telecommunications Industry (GAO/AIMD-99-293, September 30, 1999)

GSA's Effort to Develop Year 2000 Business Continuity and Contingency Plans for Telecommunications Systems (GAO/AIMD-99-201R, June 16, 1999)

Year 2000 Computing Crisis: Telecommunications Readiness Critical, Yet Overall Status Largely Unknown (GAO/T-AIMD-98-212, June 16, 1998)

Power Generation and Distribution

Y2K Computing Challenge: Nuclear Power Industry Reported Nearly Ready; More Risk Reduction Measures Can Be Taken (GAO/T-AIMD-00-27, October 26, 1999)

Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999)

Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999)

Year 2000 Readiness: NRC's Proposed Approach Regarding Nuclear Powerplants (GAO/AIMD-98-90R, March 6, 1998)

Safety and Emergency Services

Year 2000 Computing Challenge: FBI Needs to Complete Business Continuity Plans (GAO/AIMD-00-11, October 22, 1999)

Year 2000 Computing Challenge: DEA Has Developed Plans and Established Controls for Business Continuity Planning (GAO/AIMD-00-8, October 14, 1999)

Emergency and State and Local Law Enforcement Systems: Committee Questions Concerning Year 2000 Challenges (GAO/AIMD-99-247R, July 14, 1999)

Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999)

Year 2000 Computing Crisis: Status of Bureau of Prisons' Year 2000 Efforts (GAO/AIMD-99-23, January 27, 1999)

Water

Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999)

Transportation

Year 2000 Computing Challenge: FAA Continues to Make Important Strides, But Vulnerabilities Remain (GAO/T-AIMD-99-285, September 9, 1999)

Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999)

Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999)

Status Information: FAA's Year 2000 Business Continuity and Contingency Planning Efforts Are Ongoing (GAO/AIMD-99-40R, December 4, 1998)

Responses to Questions on FAA's Computer Security and Year 2000 Program (GAO/AIMD-98-301R, September 14, 1998)

FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998)

Air Traffic Control: FAA Plans to Replace Its Host Computer System Because Future Availability Cannot Be Assured (GAO/AIMD-98-138R, May 1, 1998)

Year 2000 Computing Crisis: FAA Must Act Quickly to Prevent Systems Failures (GAO/T-AIMD-98-63, February 4, 1998)

FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998)

Health

Year 2000 Computing Challenge: Compliance Status Information on Biomedical Equipment (GAO/T-AIMD-00-26, October 21, 1999)

Reported Medicaid Year 2000 Readiness (GAO/AIMD-00-22R, October 5, 1999)

Year 2000 Computing Challenge: HCFA Action Needed to Address Remaining Medicare Issues (GA0/T-AIMD-99-299, September 27, 1999)

Year 2000 Computing Crisis: Status of Medicare Providers Unknown (GAO/AIMD-99-243, July 28, 1999)

Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999)

Year 2000 Computing Challenge: Much Biomedical Equipment Status Information Available, Yet Concerns Remain (GAO/T-AIMD-99-197, May 25, 1999)

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, April 27, 1999)

Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999)

Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999)

Year 2000 Computing Crisis: Medicare and the Delivery of Health Services Are at Risk (GAO/T-AIMD-99-89, February 24, 1999)

Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998)

Year 2000 Computing Crisis: Leadership Needed to Collect and Disseminate Critical Biomedical Equipment Information (GAO/T-AIMD-98-310, September 24, 1998)

Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998)

Veterans Health Administration Facility Systems: Some Progress Made In Ensuring Year 2000 Compliance, But Challenges Remain (GAO/AIMD-98-31R, November 7, 1997)

Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses (GAO/AIMD-97-78, May 16, 1997)

Medicare Transaction System: Serious Managerial and Technical Weaknesses Threaten Modernization (GAO/T-AIMD-97-91, May 16, 1997)

Revenue Collection

IRS' Year 2000 Efforts: Actions Are Under Way to Help Ensure That Contingency Plans Are Complete and Consistent (GAO/GGD-99-176, September 14, 1999)

Year 2000 Computing Crisis: Customs is Making Good Progress (GAO/T-AIMD-99-225, June 29, 1999)

Tax Administration: IRS' Fiscal Year 2000 Budget Request and 1999 Tax Filing Season (GAO/T-GGD/AIMD-99-140, April 13, 1999).

Year 2000 Computing Crisis: Customs Has Established Effective Year 2000 Program Controls (GAO/AIMD-99-37, March 29, 1999)

IRS' Year 2000 Efforts: Status and Remaining Challenges (GAO/T-GGD-99-35, February 24, 1999)

Year 2000 Computing Crisis: Customs Is Effectively Managing Its Year 2000 Program (GAO/T-AIMD-99-85, February 24, 1999)

Internal Revenue Service: Impact of the IRS Restructuring and Reform Act on Year 2000 Efforts (GAO/GGD-98-158R, August 4, 1998)

IRS' Year 2000 Efforts: Business Continuity Planning Needed for Potential Year 2000 System Failures (GAO/GGD-98-138, June 15, 1998)

IRS' Year 2000 Efforts: Status and Risks (GAO/T-GGD-98-123, May 7, 1998)

Tax Administration: IRS' Fiscal Year 1999 Budget Request and Fiscal Year 1998 Filing Season (GAO/T-GGD/AIMD-98-114, March 31, 1998)

Benefit Payments

Year 2000 Computing Challenge: Update on the Readiness of the Department of Veterans Affairs (GAO/T-AIMD-00-39, October 28, 1999)

total of 32,598 products.[74] Of these products, 17,505 were reported as not employing a date, 9,585 were reported as compliant, 4,053 were shown as not compliant, and the compliance status of 1,455 was unknown.

In addition to the establishment of a clearinghouse, our September 1998 report[75] also recommended that HHS and the Department of Veterans Affairs take prudent steps to jointly review manufacturers' test results for critical care/life support biomedical equipment. We were especially concerned that the departments review test results for equipment previously deemed to be noncompliant but now deemed by manufacturers to be compliant, or equipment for which concerns about compliance remained. In May 1999, the Food and Drug Administration, announced that it planned to develop a list of critical care/life support medical devices and the manufacturers of these devices, select a sample of manufacturers for review, and hire a contractor to develop a program to assess manufacturers' activities to identify and correct Year 2000 problems for these medical devices. In addition, if the results of this review indicated a need for further review of manufacturer activities, the contractor would review a portion of the remaining manufacturers not yet reviewed.

The Food and Drug Administration identified 90 types of products that it refers to as computer-controlled, potentially high-risk devices, and identified 803 manufacturing sites that produce equipment sold in the United States. Of these sites, a Food and Drug Administration contractor completed 80 site visits and had prepared 62 assessment reports. We reviewed 25 manufacturer site visit reports that were completed by the examiners and available to us as of September 10, 1999. For 20 of these assessments, the examiners' assessed concern was low. At the 5 remaining manufacturers' sites, the examiner found at least one item of moderate concern, such as test planning and

[74]Because of limitations in many of the manufacturers web sites, our ability to determine the total number of biomedical equipment products reported and their compliance status was impaired. Accordingly, the actual number of products reported by the manufacturers could be significantly higher than the 32,598 products that we counted.
[75]GAO/AIMD-98-240, September 18, 1998.

Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997)

Veterans Affairs Computer Systems: Action Underway Yet Much Work Remains To Resolve Year 2000 Crisis (GAO/T-AIMD-97-174, September 25, 1997)

Veterans Benefits Computer Systems: Uninterrupted Delivery of Benefits Depends on Timely Correction of Year-2000 Problems (GAO/T-AIMD-97-114, June 26, 1997)

Veterans Benefits Computer Systems: Risks of VBA's Year-2000 Efforts (GAO/AIMD-97-79, May 30, 1997)

National Security

Year 2000 Computing Challenge: State and USAID Need to Strengthen Business Continuity Planning (GAO/T-AIMD-00-25, October 21, 1999)

Defense Computers: DOD Y2K Functional End-to-End Testing Progress and Test Event Management (GAO/AIMD-00-12, October 18, 1999)

Nuclear Weapons: Year 2000 Status of the Nation's Nuclear Weapons Stockpile (GAO/RCED-99-272R, August 20, 1999)

Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing (GAO/AIMD-99-172, June 30, 1999)

Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999)

Defense Information Management: Continuing Implementation Challenges Highlight the Need for Improvement (GAO/T-AIMD-99-93, February 25, 1999)

Defense Computers: DOD's Plan for Execution of Simulated Year 2000 Exercises (GAO/AIMD-99-52R, January 29, 1999)

Year 2000 Computing Crisis: State Department Needs To Make Fundamental Improvements To Its Year 2000 Program (GAO/AIMD-98-162, August 28, 1998)

Defense Computers: Year 2000 Computer Problems Put Navy Operations At Risk (GAO/AIMD-98-150, June 30, 1998)

Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998)

Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998)

Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998)

Defense Computers: Technical Support Is Key to Naval Supply Year 2000 Success (GAO/AIMD-98-7R, October 21, 1997)

Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues (GAO/AIMD-97-149, September 26, 1997)

Defense Computers: SSG Needs to Sustain Year 2000 Progress (GAO/AIMD-97-120R, August 19, 1997)

Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort (GAO/AIMD-97-112, August 13, 1997)

Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems (GAO/AIMD-97-106, August 12, 1997)

Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem (GAO/AIMD-97-117, August 11, 1997)

Other Government Services

Year 2000 Computing Challenge: Financial Management Service Has Established Effective Year 2000 Testing Controls (GAO/AIMD-00-24, October 29, 1999)

Year 2000 Computing Challenge: SBA Needs to Strengthen Systems Testing to Ensure Readiness (GAO/AIMD-99-265, August 27, 1999)

Year 2000 Computing Challenge: OPM Has Made Progress on Business Continuity Planning (GAO/GGD-99-66, May 24, 1999)

Year 2000 Computing Crisis: USDA Needs to Accelerate Time Frames for Completing Contingency Planning (GAO/AIMD-99-178, May 21, 1999)

Year 2000 Computing Challenge: Time Issues Affecting the Global Positioning System (GAO/T-AIMD-99-187, May 12, 1999)

U.S. Postal Service: Subcommittee Questions Concerning Year 2000 Challenges Facing the Service (GAO/AIMD-99-150R, April 23, 1999)

Department of Commerce: National Weather Service Modernization and NOAA Fleet Issues (GAO/T-AIMD/GGD-99-97, February 24, 1999)

Year 2000 Computing Crisis: Challenges Still Facing the U.S. Postal Service (GAO/T-AIMD-99-86, February 23, 1999)

Year 2000 Computing: EFT 99 Is Not Expected to Affect Year 2000 Remediation Efforts (GAO/AIMR-98-272R, August 28, 1998)

Year 2000 Computing Crisis: USDA Faces Tremendous Challenges in Ensuring That Vital Public Services Are Not Disrupted (GAO/T-AIMD-98-167, May 14, 1998)

Department of the Interior: Year 2000 Computing Crisis Presents Risk of Disruption to Key Operations (GAO/T-AIMD-98-149, April 22, 1998)

State and Local Government

Year 2000 Computing Challenge: Readiness of Key State-Administered Federal Programs (GAO/T-AIMD-00-9, October 6, 1999)

Year 2000 Computing Challenge: Status of the District of Columbia's Efforts to Renovate Systems and Develop Contingency and Continuity Plans (GAO/T-AIMD-99-297, September 24, 1999)

Year 2000 Computing Challenge: The District of Columbia Cannot Reliably Track Y2K Costs (GAO/T-AIMD-99-298, September 24, 1999)

Reported Year 2000 (Y2K) Readiness Status of 25 Large School Districts (GAO/AIMD-99-296R, September 21, 1999)

Year 2000 Computing Challenge: Readiness Improving Yet Essential Actions Remain to Ensure Delivery of Critical Services (GAO/T-AIMD-99-268, August 17, 1999)

Year 2000 Computing Challenge: Important Progress Made, But Much Work Remains to Avoid Disruption of Critical Services (GAO/T-AIMD-99-267, August 14, 1999)

Year 2000 Computing Challenge: Important Progress Made, Yet,Much Work Remains to Ensure Delivery of Critical Services (GAO/T-AIMD-99-266, August 13, 1999)

Reported Y2K status of the 21 Largest U.S. Cities (GAO/AIMD-99-246R, July 15, 1999)

Year 2000 Computing Challenge: Federal Efforts to Ensure Continued Delivery of Key State-Administered Benefits (GAO/T-AIMD-99-241, July 15, 1999)

Year 2000 Computing Challenge: Important Progress Made, Yet Much Work Remains to Avoid Disruption of Critical Services (GAO/T-AIMD-99-234, July 9, 1999)

Year 2000 Computing Challenge: Readiness Improving Yet Avoiding Disruption of Critical Services Will Require Additional Work (GAO/T-AIMD-99-233, July 8, 1999)

Year 2000 Computing Challenge: Readiness Improving But Much Work Remains to Avoid Disruption of Critical Services (GAO/T-AIMD-99-232, July 7, 1999)

Year 2000 Computing Challenge: Delivery of Key Benefits Hinges on States' Achieving Compliance (GAO/T-AIMD/GGD-99-221, June 23, 1999)

Year 2000 Computing Crisis: Readiness Improving But Much Work Remains To Ensure Delivery of Critical Services (GAO/T-AIMD-99-149, April 19, 1999)

Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999)

Year 2000 Computing Crisis: The District of Columbia Remains Behind Schedule (GAO/T-AIMD-99-84, February 19, 1999)

Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998)

Year 2000 Computing Crisis: The District of Columbia Faces Tremendous Challenges in Ensuring That Vital Services Are Not Disrupted (GAO/T-AIMD-99-4, October 2, 1998)

Year 2000 Computing Crisis: Severity of Problem Calls for Strong Leadership and Effective Partnerships (GAO/T-AIMD-98-278, September 3, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Reduce Likelihood of Adverse Impact (GAO/T-AIMD-98-277, September 2, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Mitigate Risks (GAO/T-AIMD-98-276, September 1, 1998)

Year 2000 Computing Crisis: Avoiding Major Disruptions Will Require Strong Leadership and Effective Partnerships (GAO/T-AIMD-98-267, August 19, 1998)

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Address Risk of Major Disruptions (GAO/T-AIMD-98-266, August 17, 1998)

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Mitigate Risk of Major Disruptions (GAO/T-AIMD-98-262, August 13, 1998)

Cross-Cutting Issues

Year 2000 Computing Challenge: Federal Business Continuity and Contingency Plans and Day One Strategies (GAO/T-AIMD-00-40, October 29, 1999)

Y2K Computing Challenge: Day One Planning and Operations Guide (GAO/AIMD-10.1.22, October, 1999)

Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences (GAO/AIMD-00-1, October 1, 1999)

Year 2000 Computing Challenge: Agencies' Reporting of Mission-Critical Classified Systems (GAO/AIMD-99-218, August 5, 1999)

Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999).

Year 2000 Computing Crisis: Costs and Planned Use of Emergency Funds (GAO/AIMD-99-154, April 28, 1999)

Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, November 1998)

Year 2000 Computing Crisis: Status of Efforts to Deal With Personnel Issues (GAO/AIMD/GGD-99-14, October 22, 1998)

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, August 1998)

Year 2000 Computing Crisis: Actions Needed on Electronic Data Exchanges (GAO/AIMD-98-124, July 1, 1998)

Year 2000 Computing Crisis: Testing and Other Challenges Confronting Federal Agencies (GAO/T-AIMD-98-218, June 22, 1998)

GAO Views on Year 2000 Testing Metrics (GAO/AIMD-98-217R, June 16, 1998)

Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997)

(511813)

Joel C. Willemssen

Mr. Willemssen is Director, Civil Agencies Information Systems, within GAO's Accounting and Information Management Division. In this position he is responsible for GAO's reviews of information technology management at many of the federal government's major departments and agencies, including the Departments of Agriculture, Education, Energy, Health and Human Services, HUD, Interior, Labor, Transportation, Veterans Affairs; and EPA and SSA.

Mr. Willemssen joined GAO in 1979, and since that time has participated in and led numerous computer systems reviews in a wide array of federal agencies. His evaluation experience is predominantly in assessing major modernization efforts, telecommunications, software management, performance evaluation, requirements management, acquisition approaches, systems maintenance, and business process reengineering.

Mr. Willemssen has received many awards throughout his career, including GAO's Meritorious Service Award. He received bachelor's and master's degrees in business administration from the University of Iowa, and has completed the executive level program in information systems at UCLA.

Chairwoman MORELLA. Thank you, Mr. Willemssen.

I know that Mr. Koskinen is going to have to leave us soon, and we have another vote.

Mr. KOSKINEN. No, I am actually here till 3:30.

Chairwoman MORELLA. Till 3:30. Very good. I guess I will start off with the concept that I have heard from some quarters, that there has been a little criticism from the Y2K community, maybe because you represent the Government, but the criticism has been that you have been overly optimistic about your assessments and that what you say should sort of be taken with a grain of salt. I wonder, how do you respond to those critics? You base a lot of your assessments on self-reporting. I wonder how much faith do you have in these self-reported data, and picking up also on what Mr. Willemssen had said about the areas of education and health.

Mr. KOSKINEN. Well, there are a few things to note. First of all, there is a very small minority of people out there who are in the activist community who do think that, in fact, we are going to confront much greater damage and challenges than the evidence supports. None of those people have any evidence that disputes any of the surveys that have been presented, any of the information provided by the private sector or the Government.

So, at this point, our view is, and continues to be, that we have an obligation to the public to provide them all the information we have, the good information and the areas we are troubled about. Those who have been concerned about whether we are too overly optimistic have been unhappy that we think that the critical infrastructure in this country, indeed, is going to work. Power, telecommunications, banking, finance, air traffic systems, all have been demonstrated to be ready.

But they have ignored the fact that we have in fact for some time, certainly in the last year, have been pointing to areas where we are concerned. We have been concerned about developing countries abroad, as Mr. Willemssen has noted, we have been concerned about and our surveys have demonstrated the risks involved in smaller institutions in health care and education, in small businesses, at the local government level. So that I think what you have to do is take with a grain of salt those people who are concerned about whether we are over optimistic or under optimistic.

The real issue is what are the facts as we know them, what are the facts as industries have them, and then people need to respond accordingly. Our view has been all we are doing is telling you what we know, what we have been told. I talked in my prepared statement and my oral statement about why we have reasonable confidence in the survey data that has been provided because it has been provided confidentially. And as noted, if people were going to make it up, they would have made up total compliance some time ago, and the surveys have not done that.

Chairwoman MORELLA. I do notice that organizations, businesses, and even communities are coming out with their Y2K checklists, and obviously we have yours. I received one recently from an area that I represent. It is a little bit troublesome the list of items that they say one must need. You must change from standard incandescence to compact fluorescence and halogen, replace all appliances' solar panels and wind generators, composting

toilets, reflector-powered ovens, crank-powered radio, et cetera. It goes on and on with a whole list of things.

Do you think, again on the other side, that there are areas or people that are actually contributing to panic?

Mr. KOSKINEN. Well, there are clearly those from the start, over the last 3 to 4 years, who have for one reason or another been predicting the end of the world as we know it on the ground that this is a massive problem, which indeed it is, but their prediction has been we will never be able to solve it. My disagreement with them has not been that it is a massive problem, it has been with whether we will be able to solve it.

I think there are still people pushing that if you do not buy a lot in New Mexico and leave town, at a minimum, you ought to be prepared with three to six months supplies, which I think there is no evidence to support. On the other hand, there are concerned civic groups that think that more than 3 days supplies are necessary.

Our view has been, and our brochure talks about, at least 3 days supply. And we stress that people need to take a look at their own circumstances. In the community conversations we have run across the United States, when I was in Miami, there they were talking about preparations of 7 to 10 days because that is their experience with hurricanes. In Los Angeles, their standard is a week.

What we have said is everyone needs to take a look at what their own personal situation is, what the situation is where they live. If you are in a rural community and it takes longer to find you, you will have a different approach to it. If you live in Minnesota, your approach will be different than if you are in Florida.

And so what we think is important, again, is for everybody to decide in light of the facts as they see them what they feel most comfortable about. Clearly, we think if the whole country decided that they wanted to at the last minute have months of supplies of food and water, or in fact take a lot of other activities, that by itself could create a problem where there is no basis for one.

Chairwoman MORELLA. You have been trying to create a balance, I can see.

Mr. Wu, the gentleman from Oregon, who is on our subcommittee, may not be able to return after the next vote. So I am going to let him ask a question.

Mr. WU. Thank you, Madam Chairwoman.

I would like to ask the panel, as you all know, the Securities and Exchange Commission has for some time required that private companies which are publicly held make disclosure of Y2K vulnerability in their annual statements on form 10K. How satisfied are you that these publicly held companies have, as they say, made full and fair disclosure of their Y2K vulnerabilities under the circumstances as warranted?

Mr. KOSKINEN. We have not made a judgement about that. We have not reviewed those in any detail. We have been more comfortable and confident with the information we have collected through the industry associations because, again, that is information provided with a guarantee under the statute that it is confidential, it cannot be reached by litigants or even the Federal Government.

There is a dispute, some companies are held up as models of disclosure in the SEC filings, others are held up as models of obfuscation. I think it obviously runs across the spectrum. But the judgements about the adequacy of that I think are appropriate judgements for the SEC to make since it is their regulations and their filings.

Mr. Willemssen may have a different view.

Mr. WILLEMSSEN. Congressman, we have not done an analysis of those submissions. So I am not in a position to address that question.

Chairwoman MORELLA. Gentlemen, we are going to recess for probably about 15 minutes and then we will return.

[Recess.]

Chairwoman MORELLA. The subcommittee will come to order.

I would now like to recognize Mr. Bartlett for his questioning.

Mr. BARTLETT. Thank you very much.

When you listed the items that you suggested people have in preparation, I noticed it was food and water primarily. January 1 is in the northern part of our country very cold. It is also just a few days after the shortest day in the year, with a lot of darkness. A few flashlight batteries probably will not suffice. What advice do you give relative to heat and light?

Mr. KOSKINEN. At this point, we do not advise anybody to take power into their own hands and go buy generators, again, unless you are out in the rural area, if you are at risk in the winter time from long term power outages. If Y2K is the first time you ever decide to deal with that, that is important to do it. But we do not think, in light of what we know, that there is any risk.

The power industry will operate that weekend normally at 50 percent of capacity. They will have all of the capacity or most of it spinning that weekend. So we can lose a lot of power companies, which we do not expect to lose any of them, before we will run out of power. The oil and gas industry is basically at close to 95 percent done with their work. They will, in fact, have oil and gas readily available.

So, at this juncture, we do not see any indication that we are going to have any outages, there will be glitches, that will last more than a few minutes. So the question about what happens if the power goes out in the winter time is a long term question people need to address regularly. We have ice storms and blizzards and your chances of having power outages are, in fact, greater I think because of an ice storm or a blizzard than Y2K.

And the question is "What do you do in those circumstances in your communities?" There have been places in the United States in the northeast in blizzards and ice storms that have had power outages for days rather than hours. And the answer is whatever their emergency plans and backup systems are for those situations obviously would be applicable here. We do not think there is a Y2K necessity to change to deal with those issues beyond what you normally deal with.

Mr. BARTLETT. My personal feeling is that it will come and go and we will hardly notice it. But I also think that tonight will come and go and my house will not burn. But still I have fire insurance

on my house. So as a prudent person, I think it is incumbent on us to have the equivalent of fire insurance for this possibility.

Looking at it that way, what would you say would be the equivalent of the fire insurance policy you have on your home for Y2K?

Mr. KOSKINEN. We think the equivalent of fire insurance on your home is the checklist we have put out. Again, as I say, if you think you are at risk of power going out, I think your greater risk is in an ice storm and you ought to be prepared for this weekend the same way you are prepared for the possibility of an ice storm. What happens in ice storms is people go to shelters, power is usually not out everywhere and they go to places where there is power. We have not had a problem from any of the great blizzards or ice storms in this country with people suffering because of the lack of heat or power. And whatever those processes are, the emergency managers around the United States are prepared with their normal precautions. We have, in fact, been in close contact with them and they are prepared to respond as they always do in the winter time if there are any outages.

Mr. BARTLETT. What concerns many people about the power grid is that it tends to fall back on itself. A minor problem in one place can, like dominoes, cause major problems in other places—the great northeast blackout and subsequent blackouts that were supposed to be fixed and could not happen, yet they did happen.

Do we have contingency plans so that this kind of thing will not happen?

Mr. KOSKINEN. The power industry is prepared. As I say, first of all, we will have substantial excess capacity. In fact, if there is any challenge to the grid, it will be lowered load demand rather than increased load demand to make sure we have stability. They, as I say, will have most of their systems spinning, not producing power on the grid but basically available to fill in if need be. They will make sure that there is room on the transmission lines to transmit power from area to area in case there is any need for that to be done. So they, in fact, have run two national contingency plan exercises testing how to run power plants without telecommunications, what their other contingency plans are, and they have gone through all of that with virtually every major power company in the United States in April and September. They are extremely confident. Their business is reliability. Their responsibility is responding to emergencies. And they are prepared to do that.

Mr. BARTLETT. How do they simulate the embedded chip problem? I understand with computers, we should be having some problems now because of Y2K because many computers are looking ahead several months.

Mr. KOSKINEN. Right.

Mr. BARTLETT. I am not seeing any problem, so I suspect that in terms of the programming that has been pretty well fixed. But what about the concern about embedded chips where there is no way to test them ahead of time? If it is a generic chip and you are not using the time function, that if it has a date code in it, the chip, as I understand, could shut down anyhow. How are they testing for embedded chips? And are they prepared to wire around these tens of thousands of embedded chips that are in components that they really cannot test for?

Mr. KOSKINEN. Embedded chips have been an issue that the industries generally, in addition to electric power, have been focused on. At this point, no one has found an example even though the web pages and the doomsayers continue to say there are functions in there for clocks that even if you are not using them are going to shut you down. No one yet has been able to provide a case where functionality not being used actually shut the production down. And in fact, the power companies have not found a Y2K problem failure that would shut down production.

But what they are all doing is they have reviewed those chips, they know where they are. They have reviewed them with manufacturers. Wherever they can, they have rolled the control systems and other systems forward to see what will happen. But the bottom line is, the reason we are all talking about nobody can guarantee perfection, is until we actually roll through either Greenwich Mean Time—some are set by Greenwich Mean Time, some are set on midnight—until we roll through those, we will not be able to conclusively demonstrate there is no problem. But at this point, I would stress no one has reported a problem where you could track it to a system that had that hidden clock problem that you are talking about.

Mr. BARTLETT. Greenwich Mean Time is 7 p.m. here, is that correct?

Mr. KOSKINEN. It is 7 p.m. New Year's Eve.

Mr. BARTLETT. So if there is going to be an embedded chip problem, you will expect it at 7 p.m., and not midnight?

Mr. KOSKINEN. No. It depends on how the systems are structured and where they take their time derivation.

Mr. BARTLETT. But for all of those chips that have Greenwich Mean Time, it will be 7 p.m.?

Mr. KOSKINEN. It will be 7 p.m. So, 7 p.m. New Year's Eve we will know a lot. We will actually know a lot starting at 7 a.m., New Year's Eve because New Zealand will go into the Year 2000 at 7 a.m., Australia will go at 9 a.m., and we will monitor how the world is doing. And if there are going to be systemic problems, we will have plenty of warning in terms of whether they are systemic and occurring.

Mr. BARTLETT. My last question. Several months ago the power industry testified before this committee. They told us then that because of the tens of thousands of embedded chips that they probably would not be ready, but they were sure they could wire around it. Has that changed?

Mr. KOSKINEN. All I know is what the public information surveys from them are, and that is that they are prepared. They think that they have done now 100 percent of their work, including looking and working on embedded chips and being able to respond. And we have no information that any power company is not prepared for the rollover.

Mr. BARTLETT. Thank you very much.

Chairwoman MORELLA. Thank you, Mr. Bartlett.

I now want to ask Mr. Baird from the State of Washington if he wants to ask any questions.

Mr. Baird.

Mr. BAIRD. Thank you, Madam Chair.

One of the concerns I have is I sort of did a mental checklist of my district and said what are the various potential problems. For example, we have large chemical manufacturing plants not that far away from residential areas. And one of the questions I had was let us suppose the worst case scenario; let's suppose a power outage comes along that impairs certain procedural machines or something within the chemical processor, they begin to have a breakdown, dangerous chemicals are released into the environment, we have got communications problems and transportation problems. I am not a doomsdayist by any means, but if I were a local community, I would like to have run through those various scenarios.

To what extent do you believe local communities have done that? And what should we do if they have not done it yet?

Mr. KOSKINEN. I think some communities have and, unfortunately, some communities have not. We held a White House Round Table on chemical manufacturing. We had a press conference, it produced a lot of information. We are trying to reach out. I have written a personal letter to every Governor in the United States drawing their attention to the problem, to the programs that California and New Jersey have for reaching out to the local levels.

But, clearly, it is exactly as you note, an emergency preparedness problem at the local level. We have encouraged the companies to be in touch with their local emergency planners. But the local emergency managers and public officials need to make sure that they know, they should know beyond Y2K purposes, where those plants are, what the emergency preparedness is, and, most importantly I think, is to ensure that people are on alert over that weekend and people know immediately how to get in touch with each other and what the plans are if there are any difficulties, whether, again, it is from Y2K or for some other purpose.

Mr. BAIRD. I personally see Y2K as a potential benefit in the sense that it helps us improve our emergency readiness. Are there particular checklists or steps they should go through, for example, a community working with the chemical industry and how would we get hold of that for our own districts?

Mr. KOSKINEN. EPA and the chemical manufacturers produced a manual of the items that are at risk for a smaller chemical facility that they should be checking. That is available on the EPA web site. I am sure you can get that through the Council web site of www.Y2K.gov. That material has been provided to every State. FEMA and the emergency managers have it. So I think my suggestion to a community would be their local emergency manager should contact their State or FEMA to get any additional scenario development or testing that should go on so they can ensure that they are ready for that particular kind of problem.

And I think you are right, the emergency managers across the United States think that Y2K is a great opportunity for individuals as well as organizations to review their emergency planning and preparedness and, in fact, to be better prepared than they may have been generally.

Mr. BAIRD. Thank you very much. Thank you, Madam Chair.

Chairwoman MORELLA. Thank you, Mr. Baird.

Mr. Ose, do you have any questions? As a matter of fact, before we ask that question, I was on a panel with a Red Cross represent-

ative who said, and you reminded me of it, Mr. Baird, is that what we should have on hand is what we should always have on hand.

Mr. KOSKINEN. Right.

Chairwoman MORELLA. I think that is something that makes us take inventory.

Mr. Ose from California.

Mr. OSE. Thank you, Madam Chair.

A couple of questions. Some weeks ago we had a hearing, I think Mr. Willemssen was there, regarding the FAA and the relative responses we have had from some of our international partners. At that time, we were able to ferret out information about a number of countries that had not yet responded to our Y2K circular questioning their preparedness or inquiring of it. I think the total number of countries at that time was 34 or 35. I am curious whether or not there has been any update to that list of 34 or 35.

Mr. KOSKINEN. There has been. The Department of Transportation and the FAA both have web sites now listing the information they have about preparedness internationally as well as domestically. I do not know what the number now is, but there has been an increase in the response. Transportation has now been able to categorize the nature of those responses and any concerns they have about particular airports so that the public or travel agents have direct access to that.

Mr. OSE. Madam Chair, the reason I bring this up is I want to take a moment, and I hope no one falls over here in shock, I want to take a moment to express my appreciation to Mr. Koskinen and Mr. Willemssen and the others who work in the Federal Government because we had this hearing on like a Tuesday or a Wednesday and we were asking for this information, and the agencies of the Federal Government, in response to the requests from Members of Congress, were able by Friday to refine the list from approximately 110 countries to 34 or 35 that had not responded.

The reason that is important is that, as with many people, my wife and I travel a great deal, and people in the United States travel a great deal. And the uncertainty that existed prior to the refinement of that list relative to these 70 or 80 other countries that were on the list were creating quite a bit of havoc relative to people's travel plans because they need to plan ahead, sometimes as much as 90 to 120 days.

So I want to take this moment to express my appreciation to these two gentlemen and to the others who could not join us today for making that list public, for helping the American public define where it might be safe to go and where it might not be safe to go. They really did the people's business and they deserve our applause, wherever you call it.

The FAA does have a web site on which this data is posted. If I understand correctly, it is fly2K.gov?

Mr. KOSKINEN. Correct.

Mr. OSE. I would encourage everyone to visit that who is planning on traveling over the turn of the millennium.

And, finally, one little tidbit, Madam Chair, if I could. The businesses that I used to run before I came to Congress, we have any number of security features in each of those businesses. We did a little test of our own about our Y2K preparedness. We, in effect,

took the calendars on our computers and rolled them forward to where they were like five minutes prior to midnight on the 31st and we were essentially doing our self-testing. And to those people who have not done that, I would encourage you to do that now rather than wait until the last week of December. We were fortunate. We were in compliance. But it is just a little self-test everybody might engage in.

With that, I yield back.

Chairwoman MORELLA. Thank you, Mr. Ose. And you reflect the views of both subcommittees in commendation to the agencies, Mr. Koskinen, and Mr. Willemssen, and all of the others that responded so promptly. I think we have all found that to be the case.

I am now pleased to recognize Ms. Rivers, the gentlewoman from Michigan.

Ms. RIVERS. Thank you, Madam Chair.

I have only a very brief question. There are a number of materials that are interesting and useful here in preparation and also the GAO information on evaluating how things are going. Most of us have web sites that our constituents visit on a regular basis. Are we free to link to your web sites or to use any of these materials on our sites?

Mr. KOSKINEN. We would be delighted to have you link. We would be delighted to have you take anything on the web site and put it on your web site.

Ms. RIVERS. Okay. Mr. Willemssen?

Mr. WILLEMSSEN. Certainly.

Ms. RIVERS. Great. Thank you.

Chairwoman MORELLA. Thank you, Ms. Rivers.

I am now pleased to recognize Mrs. Biggert, the gentlewoman from Illinois.

Mrs. BIGGERT. Thank you, Madam Chair.

If I might ask unanimous consent to enter my statement into the record.

Chairwoman MORELLA. Without objection, so ordered. I am also going to, without objection, have Chairman Horn's opening statement included in the record.

[The prepared statements of Hon. Judy Biggert and Hon. Stephen Horn follow:]

Opening Statement of Representative Judy Biggert (R-IL)
Government Reform Subcommittee on Government Management, Information & Technology
Hearing on Y2K Myths & Realities
November 4, 1999

Good Afternoon, Chairman Horn and Chairwoman Morella. Thank you for holding this hearing.

I understand this is to be the final formal hearing of the House Y2K Task Force before the Year 2000 arrives. As such, I want to recognize your excellent work over the last three years in raising awareness of and highlighting potential problems relating to the Year 2000 date change.

Although I have been a member of the Subcommittee and the Y2K Task Force for less than a year, I know the amount of time and resources that you and your staff have dedicated to this important matter. You are to be commended for this effort, particularly for the progress that has been made on this issue just in the last year.

Since January, we've discussed the impact Y2K could have on commerce, government services, transportation, health, national security, as well as the impact it could have in our own homes. But as much as we have raised the public's understanding of this issue, many questions and concerns – some justified, some not – still remain.

That's why we are here today – to work through the outstanding issues and to sort out what is Y2K myth and what is Y2K reality. We are here to help the American people understand what they should and should not expect from the so-called Millennium Bug and how they can prepare for any problems that may arise.

Polls show that a majority of Americans believe they will experience at least minor problems from the year 2000 date change. I think they are right to be a little concerned and should prepare accordingly.

What do I mean by prepare? I mean taking common sense actions, such as having extra food and water, having extra amounts of your prescription medications available, or having a little more cash on hand than usual.

Come January 1, 2000, I don't expect to hear about major disasters caused by the Y2K bug. However, we should not be so naïve to think that there won't be *any* problems or disruptions in essential services. Let us hope that the work undertaken by this Committee, by the Administration and others served to head off some of these potential disruptions, as well as helped the American public prepare for problems that do arise.

Again, Mr. and Madam Chairman, I commend you for calling this hearing and for all the work you have done on this important issue. I look forward to hearing from our witnesses and thank them for joining us today as we attempt to work through Y2K fact and fiction.

Opening Statement
Chairman Stephen Horn (R-CA)
Subcommittee on Government Management,
Information, and Technology
November 4, 1999

No one knows precisely what will happen when the clock strikes midnight on December 31, 1999. Nevertheless, predictions are springing up like wild flowers in May. Entrepreneurs are aggressively promoting their Year 2000 survival kits, attempting to cash in on products such as dried foods and home generators in case of widespread disruptions. Will the disruptions occur in the early hours of January 1, 2000? Will they occur at all? In truth, it may take days, weeks or even months to learn whether the billions of dollars it has cost to prepare public and private computer systems for the Year 2000 was money well spent.

If reports are true, the troublesome millennium bug may have been around for years. For example, in 1993, Minnesota officials instructed 104-year-old Mary Bandar to report to kindergarten. It turned out that state computers had misread Ms. Bandar's 1889 birth date as 1989, placing her age at 4. Recently in Maine, several hundred car owners were dismayed to find the titles to their new year-2000 model vehicles categorized as "horseless carriages." State computers had misread the Year 2000 as 1900, back in the days when horsepower really involved horses.

Last week, computer giant IBM reported that its computer mainframe sales had fallen because of customer concern over the Year 2000 problem. IBM's stock dropped nearly 20 percent in a single day.

At this point, the reported disruptions fall somewhere between humorous and annoying. They are hardly catastrophic. And, in fact, minor inconveniences occur every day. Whether it is a traffic jam, a cranky automated teller machine, or a cancelled airline flight -- people adjust. Recent public opinion polls support the notion that Year 2000 anxiety is waning. Indeed, if Americans are informed and prepared for Year 2000 disruptions, they will cope.

Only 57 days remain until the January 1st deadline. Today, we will discuss the nation's Year 2000 efforts -- in the Government and in the private sector. We want to hear about the remaining risks, and what steps are needed to mitigate those risks.

I welcome today's witnesses, and look forward to their testimony.

Mrs. BIGGERT. This has been an unusual day. I apologize for missing your statements. I would like to ask, have you heard rumors about Y2K that you would like to dispel? Is there something that you hear out there that you would have concern about?

Mr. KOSKINEN. I appreciate that question. In my formal statement, we have listed the myths and the rumors that generally we are concerned about. I suppose, and it goes back to the Chairwoman's question, the ultimate rumor I would like to dispel is that somehow we have information in the Federal Government or in the President's Council that we are not sharing with the public. There is no evidence, nobody has ever established something we know that we have not told. And, in fact, our strategy for now going onto 2 years has been to share with the public everything we have as we get it.

So, as I say, I think the rumor that there is this secret information that we are somehow afraid to release is just that, a rumor. Our goal in life is to have the American public feel they know everything I know and can then decide how to respond appropriately.

Mrs. BIGGERT. Okay. Mr. Willemssen?

Mr. WILLEMSSEN. I would also echo Mr. Koskinen's comment. Obviously, we come at this from an audit and evaluation perspective. We have seen all the data as best as I know that Mr. Koskinen has available. To the extent that we identify that data, we take the opportunity to publicize it in our reports and testimonies. That is why one thing we wanted to do today in our testimony was reflect the broad nature of everything we have done and the kind of progress that has been made, while at the same time pointing out some residual risks.

Mrs. BIGGERT. Certainly, we have spent a lot of time, had a lot of hearings. I would like to commend the two chairmen of these two committees for everything that they have done, and certainly started long before I got here this year, working on this.

Is there anything that you think we as the Congress have missed doing that we should have done on the Y2K problem?

Mr. KOSKINEN. I do not think so. We have had, I think the Chairwoman was right, this has been a very bipartisan issue. We have not had any concern in either house of Congress about any kind of political issues entering into this. We have had great support. We have obviously had a very good working relationship with GAO as well working on behalf of the Congress. So if we had to do it again, there is nothing that we have asked of the Congress that has not been granted to us. I think it has been a very good example of the cooperation between the legislative and the executive branch dealing with what is a serious national challenge.

Mrs. BIGGERT. Mr. Willemssen?

Mr. WILLEMSSEN. Looking forward, I would say the one thing that the Congress can still be of great benefit to the citizenry is reminding the citizens what the facts are. I think as we are into November and we turn into December, there is going to be the opportunity for some to view this in survivalist terms, if you may, that it really is going to be much worse than it actually will be. So I think the Congress can still serve a very useful role in informing the public of what the facts are, what the readiness is, where we

do have some risks, but the overriding fact is we are in a much better prepared state today than we have been.

Secondly, to the extent that problems do occur, major Federal agencies and most private organizations are planning detailed day one strategies to be prepared in the event that disruptions occur.

Mrs. BIGGERT. I think there was something in the paper the other day that everyone should not get on the phone at 12:01 to say everything is okay because it is going to jam the telecommunication lines.

Mr. KOSKINEN. That is right. We refer to it in our checklist, too. There is likely to be Mother's Day by multiples if everybody both celebrating the millennium and also just checking in does that at one time. At a minimum, what people should understand, if you do not get a dial tone immediately or you get a rapid dial, it is very likely not to be a Y2K problem but to be the fact that your neighbors and everybody else have joined you on the phone at the same time.

Mrs. BIGGERT. Right. Thank you very much for all your hard work. Thank you Madam Chairman.

Chairwoman MORELLA. Thank you, Mrs. Biggert.

Mr. KOSKINEN. Madam Chairman, I am afraid I have over 50 people on this conference call that I noted I need to join. I hate to deprive your co-chair here of his chances——

Mr. HORN. I do not think you are going to deprive me.

Mr. KOSKINEN. But I am going to have to leave. I would be happy to take a question or two, and then I am going to have to go.

Mr. HORN. Fine. All right. If you had to do it over again, when you were appointed in February 1998 and you started in April 1998, what would you advise Congress and a President to do in terms of the type of structure or communications or whatever? Say we had something similar to this where all of our computers were crashing because of people that were using sort of economic terrorism, if you will, how would you deal with that, and would you deal any differently than you have done?

Mr. KOSKINEN. I would not change, certainly for the Y2K issue, anything that we have done. I think, again, we have had great cooperation with the Congress. I think our basic approach has been validated by the amount of progress that has been made. I think there is no way, as some suggested, that we could legislate our way out of this problem, to in fact start telling everybody how to do it. What we needed to do was marshall the expertise and the energy of the people in the private sector as well as the public sector.

I think your point is well taken in terms of going forward; and that is, we are going to become more reliant, rather than less, on information technology in the future, which means we will be more vulnerable, rather than less, to terrorists, to hackers, to others who want to in fact disrupt our systems. And, therefore, I think we do need to be prepared for that. But at this juncture, I do not have a proposal as to how we ought to move from this issue to that in terms of structuring to deal with it. All I can tell you is I think the structure worked very effectively for the crisis we knew we were facing when I took on this role.

Mr. HORN. Well, in terms of getting the work done in a timely way, do you think February 1998 was a little late? And shouldn't

the early Clinton Administration and the Bush Administration been involved in this? After all, Social Security showed the way and they did 100 percent.

Mr. KOSKINEN. Well as I said when you asked me that question over a year ago, we will know the answer to that in terms of how we get through this process effectively. As I say, at this point, the Federal Government is over 99 percent done. I do not think there are any risks in the Federal processes that would have been avoided otherwise.

As you know, when I was in the Government before, we started a cross-government issue dealing with this in 1995. So that hindsight is always interesting, but at this point we do not have a view that we would be in a whole lot different shape. It might have been a little less hectic if we could have gotten people's attention. But you have to understand, as you remember when you were one of the lone voices raising this issue back when we were working on it——

Mr. HORN. April 1996. And nothing much happened until February 1998.

Mr. KOSKINEN. Yes, 1998. Well, what we both had, and I had that same experience, is in 1995 and 1996, even for people who should have known better, the year 2000 seemed like a long way off. And it was our biggest challenge, even when we all started working together in February 1998, the biggest challenge was getting people to understand they needed to pay attention to this, not just as another issue, but as their top priority in terms of the threat it made to their ability to operate. And I think you started early, the Government started early, but I think it is human nature not to focus on things any earlier than you can make people do that.

Mr. HORN. Well I know a lot of Government operates just like universities do—your neck has to be in the guillotine or you are pushed against the wall and then finally something happens.

Mr. KOSKINEN. A lot of people in the private sector still have not even gotten there yet. So it is not just a Government or university problem.

Mr. HORN. That is my next question to you.

Mr. KOSKINEN. This will have to be the last one. I really am late.

Mr. HORN. All right. In August, you reported confidence and concerns in various public and private sectors. For example, the Council expressed "High degree of confidence" in major domestic areas like financial institutions, electric power, and the Federal Government. However, the Council expressed concerns with local governments, health care, education, and small businesses.

The President's Council plans to issue its final Y2K report next Wednesday. I guess I would ask you, in foreshadowing your forthcoming report, what domestic and international areas are you still concerned with?

Mr. KOSKINEN. Again, we are pulling that report together and we still have some information being provided by some——

Mr. HORN. Just whisper me——

Mr. KOSKINEN. Just whisper any. Basically, we do not have new sectors that we are now any more concerned about than we were. What is hardest for us to measure is how much progress is being

made in the areas we are concerned about. Last week, we had an event with the Department of Education in which it was noted that educational institutions, for instance, have made substantial progress. They have gone from about a third readiness of the organizations to two-thirds, which is the good news. The bad news is that still means a third of them are not prepared at this time, both higher education and elementary and secondary.

So that I think the best way to summarize the difference between August and November will be that progress continues to be made but there are still going to be organizations that are at great risk because they are going to be talking about finishing their work in December and that does not give them any margin for error. Which means that they, of all people, need to have contingency plans and backup plans because, if you are planning to finish your work in December, there is a reasonable chance something will not work well, you will not have time to test adequately, you need to be prepared with a backup plan.

Mr. HORN. Will the Council be pushing for that right up to December 31st?

Mr. KOSKINEN. We will push testing. Our view is you need to keep working on remediation, on testing, re-testing, and on contingency plans with every day and every hour you have left in this year, even if you think you are done today.

Mr. HORN. I think you will recall a couple of months ago I sent a letter to the Secretary of Education, copied you, and talked to you about it. I have not heard much action. Is anything happening? I heard some press release or something the Secretary did that, gee, it is tough with K–12.

Mr. KOSKINEN. We have written, the Secretary and I, to every superintendent of education, every State department, we have written to local superintendents. We have had meetings since then. We have provided technical information. The Department since then has done another telecommunication to sites all around the United States. Again, at some point it is a little like our problem with some small businesses—you can lead them to water, but you cannot make them fix their systems.

Mr. HORN. Well, I was looking for the Secretary to say, look, it is going to take X amount to help K–12. Let me reprogram the money. I think Congress would have permitted him to reprogram the money. So that is what has bothered me. It just seems like a little bit of drift.

I will let you off on that happy note.

Mr. KOSKINEN. Thank you. Thank you all very much. I apologize.

Mr. HORN. We appreciate your work.

Chairwoman MORELLA. Mr. Turner will be asking his question of Mr. Willemssen.

Are you going to be the media spokesperson in the ICC?

Mr. KOSKINEN. I am going to be the media spokesperson. I will be there.

Chairwoman MORELLA. You will be the one that will contact us. We will be in touch. Thank you very much.

Mr. KOSKINEN. I get all the good jobs. Thank you all very much, and I apologize for having to leave.

Mr. HORN. Thank you, John.

Chairwoman MORELLA. Thank you for the good work that you have done. We look forward to staying in touch with you now.

Mr. Willemssen, do you mind staying here with the next panel? Would that be all right?

Mr. WILLEMSSEN. Certainly.

Chairwoman MORELLA. Excellent. Thank you. You have been very patient from the beginning to the end. Great.

I am going to ask the next panel if they would come forward. We have Mr. Campbell, Mr. Scher, Mr. Margolis. Mr. Robert Kringley, unfortunately, could not be joining us today.

And so, leading off on the second panel is Mr. Pat Campbell, the chief operating officer of the NASDAQ stock market, the largest stock market in the world in terms of dollar value of shares traded, and whose composite index hit an all time high, cresting at over 3,000 just yesterday. Mr. Campbell is going to discuss with us some of the concerns affecting investor confidence in the stock market.

Next on our panel is Mr. Barry Scher, who is the vice president of Giant Food, the largest retail food/pharmacy chain serving the mid-Atlantic region. We have asked Mr. Scher to talk about Y2K marketing and what Americans can expect as they go to the stores before and after January 1, 2000.

And rounding out our second panel is Mr. Ronald Margolis, the chief information officer of the University of New Mexico Hospital in Albuquerque. Mr. Margolis is also speaking on behalf of the American Hospital Association that represents nearly 5,000 hospitals, health systems, networks, and other providers of care. Mr. Margolis will discuss with us some of the strong Y2K collaborations with hospitals, emergency services, and the government that he helped to create in Albuquerque. He will also help us to review some of the concerns dealing with hospitals and whether Americans can expect to receive necessary medical treatment as we begin the new millennium.

Additionally, the American Medical Association has submitted written testimony. I seek unanimous consent to insert it into the record. Hearing no objections, so ordered.

[The prepared statement submitted by the American Medical Association follows:]

American Medical Association
Physicians dedicated to the health of America

1101 Vermont Avenue, NW
Washington, DC 20005

Statement

to the

**Subcommittee on Government Management,
Information and Technology
Committee on Government Reform
U.S. House of Representatives**

and

**Subcommittee on Technology
Committee on Science
U.S. House of Representatives**

RE: Y2K, Myths and Realities

November 4, 1999

Division of Legislative Counsel
202 789-7426

61-629 00 - 4

STATEMENT

of the

American Medical Association

to the

Subcommittee on Government Management, Information and Technology,
House Government Reform Committee,
and
Technology Subcommittee,
House Committee on Science

RE: Y2K, Myths and Realities

November 4, 1999

The American Medical Association (AMA) appreciates the opportunity to submit to the Subcommittee on Government Management, Information and Technology of the House Government Reform Committee, and to the Technology Subcommittee of the House Committee on Science this written statement concerning the medical profession's Y2K readiness. The AMA realizes the potential impact and seriousness of the Year 2000 problem on patients and their physicians, and we are grateful for Congress's ongoing interest in this issue.

PHYSICIANS' Y2K READINESS

The inability to process properly year 2000 date data is a serious problem for the entire health care industry, and is commonly known as the "Y2K problem" or the "Y2K bug." As reported by many sources, physicians and other health care providers may be lagging in their efforts to successfully prepare their practices for the Y2K problem.

The HCFA Administrator has urged physicians who have not taken the necessary steps, to do so, and recently provided a checklist of steps that should be followed to assure Y2K readiness. HCFA has also sent a letter to every physician submitting claims to Medicare reiterating the same message. The AMA strongly supports the Administrator's initiative to assist physicians in this area. As discussed below, the AMA has taken an active role for almost two years in helping to educate and prepare physicians for the possible problems associated with the Year 2000.

Current Level of Preparedness

The medical industry relies heavily on technology, computer systems – both hardware and software – and medical devices that have embedded microchips. A survey conducted last

year by the AMA found that almost 90 percent of the nation's physicians are using computers in their practices and 40 percent are using them to log patient histories.[1] These numbers appear to be growing as physicians seek to increase efficiency and effectiveness in their practices and when treating their patients. Physicians' dependence on technology consequently creates vulnerability to the Y2K bug.

Assessing the status of the Y2K problem has been difficult because the inventory of the information systems and equipment that will be affected is far from complete and the consequences of noncompliance for each system remain unclear. Additionally, the health care industry is extremely fragmented and consistently requires complex information transactions.[2] Due to these characteristics, physicians and other health care providers have also been unable to conduct adequate testing, particularly parallel and end-to-end testing. In fact, HCFA has stated that fewer than 2% of the more than 230,000 Medicare providers have tested their systems with Medicare contractors. HCFA further stated that of that 2%, from 10% to 30% have experienced problems.[3]

Despite the rather bleak outlook, other surveys offer some favorable information. Rx2000 Solutions Institute, a non-profit organization established to address Y2K issues in the health care industry, reports that recent data show that while Y2K progress among health care providers is lagging behind other industries, **an increasing number of providers are beginning to address the issue**. Rx2000 reports further that greater numbers of physicians and other health care providers have documented Y2K plans; currently, 76 percent of health care providers have plans for addressing the Y2K problem. Moreover, increasing numbers of physicians and other health care providers have set aside funds for Y2K remediation efforts and have begun exploring the Y2K status of their business partners.

Results from the AMA's March 1999 survey, while inconclusive due to the relatively low response rate, nevertheless **appear to confirm Rx2000's findings**. Approximately three-quarters (76 percent) of the physicians who responded have conducted an inventory of their practices to determine whether they are Y2K dependent, and 71 percent of the respondents have developed a strategy for dealing with potential Y2K information systems problems. Most important, of the physicians who reported that their practices were not currently Y2K-ready (53 percent), almost all – 94 percent – indicated that their practices will be Y2K compliant by December 31, 1999.

In September 1999, the AMA conducted a second survey, which provided very similar findings. This recent survey found that of the physicians responding, 86 percent have conducted an inventory of their practices to determine whether their practices use equipment and services that are Y2K dependent, and **three-quarters report that their practices are currently Y2K ready. Of those physicians who are not currently ready, nine out of ten**

[1] "Doctors Fear Patients Will Suffer Ills of the Millennium Bug; Many Are Concerned That Y2K Problem Could Erroneously Mix Medical Data – Botching Prescriptions and Test Results," Los Angeles Times, Jan. 5, 1999, p. A5.
[2] Violino, B., "Health Care Not Y2K-Ready—Survey Says Companies Underestimate Need for Planning; Big Players Join Forces," InformationWeek, January 11, 1999.
[3] Marwick, C., "R U E 4 Y2K?," JAMA, Vol. 282, No. 15, October 20, 1999, p. 1411.

(89 percent) indicate that their practices will be compliant by December 31, 1999. Additional surveys conducted by the General Accounting Office have provided comparable results.

With just 57 days left, the medical industry continues to diligently prepare for the new millennium. While the Senate Special Committee on Y2K reported that the health care industry significantly lags behind most other industries, it also emphasized that Americans, and patients in particular, have no reason to panic.

Given the level of uncertainty about Y2K preparedness, we reiterate the importance of our recommendations that physicians, carriers and the federal government must work together now to ensure overall compliance (especially with respect to billing procedures) and the existence of effective contingency plans.

A Collaborative Effort

Patient Care

Although it is difficult to determine the level of risk to patient safety resulting from Y2K problems, we do know that the risk is real. For example, if a Y2K problem were to cause certain imbedded microchips to malfunction, monitors relying on those microchips could fail to sound alarms when patients' hearts stopped beating. Similarly, respirators could deliver "unscheduled breaths" to respirator-dependent patients, and digital displays could incorrectly attribute the names of some patients to medical data from other patients. Further, since 1986, the FDA has received more than 450 reports identifying software defects—unrelated to Y2K—in medical devices. In one instance, a software error caused a radiation machine to deliver excessive doses to six cancer patients, resulting in three fatalities.[4]

In light of the foregoing, the AMA continues to recommend strongly that medical device manufacturers immediately disclose to the public whether their products are Y2K compliant. Only the manufacturers have the necessary in-depth knowledge of the devices they have sold. Physicians and other health care providers do not have the expertise or resources to determine reliably whether the medical equipment they possess will function properly in the year 2000.

Nevertheless, medical device manufacturers have not always been willing to assist end-users in determining whether their products are Y2K compliant. Last year the FDA estimated that only approximately 500 of the 2,700 manufacturers of potentially problematic equipment had even responded to inquiries for information. Even when vendors did respond, their responses frequently were not helpful. The Department of Veterans Affairs reported last year that of more than 1,600 medical device manufacturers it had previously contacted, 233 manufacturers did not reply and another 187 vendors said they were not responsible for alterations because they had merged, were purchased by another company, or were no

[4] Anthes, Gary H., "Killer Apps; People are Being Killed and Injured by Software and Embedded Systems," Computerworld, July 7, 1997.

longer in business. One hundred and two companies reported a total of 673 models that were not compliant but should be repaired or updated this year.[5]

The Special Committee reported that "[e]very major medical organization testified that they [sic] were experiencing significant problems with biomedical device manufacturers. In many cases, manufacturers were unable or unwilling to comment on their product's ability to function after the millennium change." Moreover, it stated that only after informing device manufacturers that Congress would enact legislation requiring mandatory disclosure if the manufacturers did not voluntarily disclose compliance information, did the manufacturers begin providing compliance data to the FDA.

We therefore urge the FDA to continue to assist physicians and other health care providers in obtaining necessary compliance information for medical devices. We also thank the FDA for identifying on its website medical devices that it believes are non-compliant and potentially dangerous. The FDA site has been an invaluable resource for physicians.

Administrative Systems

Many physicians and medical centers are increasingly relying on information systems for conducting medical transactions, such as communicating referrals and electronically transmitting prescriptions, as well as maintaining medical records. In addition, many physician and medical center networks have begun creating large clinical data repositories and master person indices to maintain, consolidate and manipulate clinical information. increase efficiency and improve patient care. If these information systems malfunction, critical data may be lost, or worse—unintentionally and incorrectly modified. Even an inability to access critical data when needed can seriously jeopardize patient safety.

Other administrative aspects of the Y2K problem involve Medicare coding and billing transactions. In January 1999, HCFA instructed both carriers and fiscal intermediaries to inform health care providers, including physicians and suppliers, that claims received on or after April 5, 1999, which were not Y2K compliant would be rejected and returned as unprocessable. HCFA has already indicated that virtually 100 percent of the electronic bills being submitted by physicians and other Medicare Part B providers already meet HCFA's Y2K filing criteria. With that hurdle successfully behind us, physicians must now focus on whether the first two digits of the century, *i.e.*, "20," will be picked up and recognized by the physician's billing service and third party payers. It is our understanding that while physicians' claims are being submitted with a four digit year – 1999 – many billing services are "correcting" how the date is reported by simply adding the first two digits of the year—"19." The concern then becomes whether the software will be capable of accurately noting the change to the 21st century. The clear answer can only be determined by testing with billing services and third party payers.

[5] Morrissey, John, and Weissenstein, Eric, "What's Bugging Providers," Modern Healthcare, July 13, 1998, p. 14. See also, July 23, 1998 Hearing Statement of Dr. Kenneth W. Kizer, Undersecretary for Health Department of Veterans Affairs, before the U.S. Senate Special Committee on the Year 2000 Technology Problem.

We genuinely hope that HCFA will continue to aggressively assist physicians and other health care professionals who thus far have been unable to achieve full Y2K compliance. We greatly appreciate HCFA's implementation of a "1-800" call-in service (1-800-958-HCFA), whereby physicians and other health care providers may seek HCFA's assistance in ensuring that their systems are Y2K compliant. We are also particularly grateful for HHS identifying November 15th through November 20th as the "National Medicare Y2K Testing Week," during which time physicians may test their forward-dated Medicare claims with their Medicare contractors. We applaud these critical initiatives, and we reiterate that physicians are genuinely trying to achieve full Y2K compliance.

Reimbursement and Implementation of BBA

To remedy its own problems, HCFA has stated it will concentrate on fixing its internal computers and systems. As a result, it will not implement some changes required under the Balanced Budget Act (BBA) of 1997, and plans to postpone physicians' payment updates from January 1, 2000, to January 17, 2000. Since HCFA had at one time indicated that it would delay payment updates by three months, we are pleased that HCFA is moving in the right direction to eliminate update delays. The AMA has previously indicated to HCFA that delays in Medicare's reimbursement updates could have consequences far beyond the Medicare program. Many private insurers and state Medicaid agencies base their fee-for-service payment systems on Medicare's RBRVS, and thus may follow HCFA's lead with respect to delays in payment updates, thereby resulting in a much broader than expected impact on physicians.

AMA Y2K COMPLIANCE ASSISTANCE EFFORTS – A CHRONOLOGY

The AMA has devoted numerous financial resources and is conducting a number of activities to assist physicians with Y2K problems, as outlined below. Indeed, AMA policy directs the AMA to study the Y2K problem and its possible adverse effects on patient care and physicians, and to educate and assist physicians in becoming Y2K compliant.

As a precursor to its Y2K remediation efforts, in early 1996, the AMA formed the National Patient Safety Foundation or "NPSF." **Our goal was to build a proactive initiative to prevent avoidable injuries to patients in the health care system.** In developing the NPSF, the AMA realized that physicians, acting alone, cannot always assure complete patient safety. In fact, the entire community of providers is accountable to our patients, and we all have a responsibility to work together to fashion a systems approach to identifying and managing risk. It was this realization that prompted the AMA to launch the NPSF as a separate organization, which in turn partnered with other health care organizations, health care leaders, research experts and consumer groups from throughout the health care sector.

One of these partnerships is the National Patient Safety Partnership (NPSP), a voluntary public-private partnership dedicated to reducing preventable adverse medical events and convened by the Department of Veterans Affairs. Other NPSP members include the American Hospital Association, the Joint Commission on Accreditation of Healthcare

Organizations, the American Nurses Association, the Association of American Medical Colleges, the Institute for Healthcare Improvement, and the National Patient Safety Foundation at the AMA. The NPSP has made a concerted effort to increase awareness of the year 2000 hazards that patients relying on certain medical devices could face at the turn of the century.

For more than a year, the AMA has also been educating physicians and medical students through two of its publications, *AMNews* and the *Journal of the American Medical Association (JAMA)*. *AMNews*, a national newspaper widely distributed to physicians and medical students, has regularly featured articles for the last nineteen months discussing the Y2K problem, patient safety concerns, reimbursement issues, Y2K legislation, and other related concerns. This publication has carried Y2K editorials, information about available resources, and other articles intended to make physicians aware of the Y2K conversion efforts that will be necessary to protect their patients and practices. The AMA has also been placing—and will continue to place—advocacy ads in *AMNews* in a further effort to bring physicians' attention to the Y2K issue.

Through these publications, the AMA has been raising the level of consciousness among physicians of the potential risks associated with the year 2000 for their practices and patients, and identifying avenues for resolving some of the anticipated problems.

The AMA has also developed a national campaign entitled "Moving Medicine Into the New Millennium: Meeting the Year 2000 Challenge," which incorporates a variety of educational seminars, assessment surveys, promotional information, and ongoing communication activities designed to help physicians understand and address the numerous complex issues related to the Y2K problem. In June 1998, the AMA launched this campaign by assembling state, county and medical specialty executives from around the country for an informational seminar, presenting an overview of the Y2K problem and its potential impact on the medical profession.

In August 1998, AMA staff met with attendees of the American Association of Medical Society Executive (AAMSE) annual meeting to discuss, answer questions regarding, and in general raise the level of physician awareness of the Y2K problem.

A seminar series sponsored by the AMA is the "Advanced Regional Response Seminars" program. We have been holding these seminars in various regions of the country and providing specific, case-study information along with practical recommendations for the participants. The seminars provide tips and recommendations for dealing with vendors and explain various methods for obtaining beneficial resource information. Seminar participants receive a Y2K solutions manual, entitled *The Year 2000 Problem: Guidelines for Protecting Your Patients and Practice*. This manual, which we have made available to hundreds of thousands of physicians across the country, offers a host of different solutions to Y2K problems that physicians will likely face. It raises physicians' awareness of the problem, year 2000 operational implications for physicians' practices, and identifies numerous resources to address the issue.

In addition to these seminars, an AMA subsidiary, AMA Solutions, Inc., has been enlisting the cooperation of physician group practices, hospitals and Federation members across the country to host Y2K presentations.

The AMA in June 1998 established a website (URL: www.ama-assn.org/not-mo/y2k/index.htm) to provide the physician community additional assistance to better address the Y2K problem. The site serves as a central communications clearinghouse, providing up-to-date information about the millennium bug, as well as a special interactive section that permits physicians to post questions and recommended solutions for their specific Y2K problems. The website contains a wealth of Y2K-related information, and includes a medical equipment inventory list as well as links to other key sites such as the FDA's. Since its inception, it has generated approximately 55,500 "hits," and we have been adding new content to generate repeat visits.

The AMA has conducted or participated in several surveys to measure the medical profession's state of readiness, assess where problems exist, and identify what resources would best reduce any risk. The AMA, along with several other national organizations, recently participated in a survey of 5,000 physicians nationwide, which was conducted by the Department of Health and Human Service's Office of Evaluations and Inspection of the Office of the Inspector General. The AMA has sought to use the information we have obtained from these surveys to identify which segments of the medical profession are most in need of assistance. We have also attempted to tailor our efforts to meet the specific needs of physicians and their patients, and to more effectively assist our constituent organizations in responding to the precise needs of other physicians across the country.

During its 1999 Annual Meeting, the AMA featured a Y2K exhibit, which drew physicians' attention to the AMA website and the AMA *Year 2000* manual. We also offered suggestions on how physicians could assess their readiness, and answered questions and encouraged them to develop detailed contingency plans. We also set up this exhibit at the Medical Group Management Association regional meetings last June and July.

In an effort to offer leadership to the Federation, the AMA has been communicating with state, county and specialty medical societies across the country, explaining the Y2K problem and urging them to alert physicians. We have offered our assistance to these societies and requested that they inform us of their efforts to assist physicians in becoming Y2K compliant.

THE CHALLENGE

Both the public and private sectors should encourage and facilitate health care practitioners in becoming more Y2K compliant and taking action to mitigate their risks. Greater efforts must be made in educating physicians, other health care providers and health care consumers about the issues concerning the year 2000, and particularly, how they can develop Y2K remediation plans, properly test their systems and devices, and accurately assess their exposure. **We urge HCFA to devote further resources to assist physicians in**

identifying Y2K compliance problems, testing equipment—which at this juncture is crucial—and in developing solutions and contingency plans to ensure patient safety.

We also recommend that communities and institutions learn from other communities and institutions that have successfully and at least partially solved the problem. Federal, state and local agencies as well as accrediting bodies that routinely address public health issues and disaster preparedness are likely leaders in this area. At the physician level, this means that public health physicians, including those in the military, organized medical staff, and medical directors, will need to be actively involved for a number of reasons. State medical societies can help take a leadership role in coordinating such assessments.

We are aware that the "Year 2000 Information and Readiness Disclosure Act" and "The Y2K Act" were recently passed and enacted into law, and are intended to restrict Y2K litigation by granting protection to certain defendants in Y2K suits. Under the former statute, protection against litigation is offered to encourage manufacturers to disclose Y2K compliance information. Although the AMA strongly believes that information must be freely shared between manufacturers and consumers, we continue to caution against providing liability caps to manufacturers in exchange for the Y2K information they may provide. As we have stated before, generally vendors alone have the information about whether their products were manufactured to comply with year 2000 data. **These manufacturers should disclose that information to their consumers without receiving an undue benefit from a liability cap.**

The latter statute offers a host of liability protections to defendants in lawsuits arising out of device, equipment, software or hardware failures caused by the "year 2000" problem. The statute, however, expressly excludes from its scope claims based on personal injury.

As you may realize, Y2K-related lawsuits against physicians and other health care providers will likely arise out of personal injury claims. Third-party actions against the manufacturers will typically arise out of or rely on a breach of contract and will not be based directly on "personal injury." Consequently, this statute will protect device and equipment manufacturers – who are the most knowledgeable about their products – while exposing to liability physicians and other providers who have little knowledge about whether the equipment is Y2K compliant. So, despite patients being injured by equipment malfunction, medical equipment manufacturers would likely enjoy many of the protections of this law. **To limit manufacturers' liability exposure under these circumstances, while leaving physicians and providers vulnerable to suits, flies in the face of sound public policy.**

We continue to stress that medical device and software manufacturers need to disclose publicly and immediately Y2K compliance information regarding products that are currently in use. Any delay in communicating this information may further jeopardize practitioners' efforts at ensuring compliance. We emphasize that at this stage, all compliance information must be accurate, complete, sufficiently detailed and readily understandable for physicians. We suggest that the federal government and Congress continue to enlist the active participation of the FDA or other government agencies in mandating appropriate reporting procedures for vendors. We applaud the Department of Veteran Affairs, the FDA, and

others who maintain Y2K web sites on medical devices and offer other resources, which have already helped physicians to make initial assessments about their own equipment.

We also must build redundancies and contingencies into the remediation efforts as part of the risk management process. Patients are vulnerable to information systems and medical equipment failures. Injuries may also be caused by physical plant equipment malfunctions—for example, by a hospital elevator that stops working properly, or a heating/ventilation/air conditioning system that fails or by an unexpected power outage. The full panoply of systems that may break down as our perception of the scope of risk expands may not be as easily delineated as the potential problems with medical devices. Building in back-up systems as a fail-safe for these unknown or more diffuse risks is, therefore, absolutely crucial.

To the extent that physicians—particularly those in small practices, and other health care providers, do not have the required capital to remedy their Y2K problems, we welcome the Small Business Administration's (SBA) efforts to ensure that loans are made available on a restricted basis for businesses to correct Y2K problems.

We must counter any possibility that the public will overreact to potential Y2K-related problems. To that end, the AMA continues to participate with the Administration and the pharmaceutical community in a process to develop interventions designed to reassure the public that the pharmaceutical supply is secure and that patient safety will be maintained as we transition into the millenium. We have also been actively participating in the "Pharmaceutical Alliance for Y2K Readiness," which is a coalition of drug manufacturers, wholesale distributors, pharmacies, and health care organizations that are working closely with government leaders to ensure that consumers retain access to a continued and substantial supply of pharmaceuticals through January 1, 2000.

From this extensive Y2K educational activity currently underway within the AMA, it should be readily apparent that we believe that physicians should be making all necessary contingency plans to protect both their patients and their practices from the Y2K computer bug. We urge you to join with us in sending the message to all physicians that there is still time to make the necessary adjustments to their practice and to develop needed contingency plans.

We appreciate the committees' interest in addressing the matters discussed in our testimony and stand ready to assist Congress in further addressing any problems related to these issues as they arise.

Chairwoman MORELLA. Gentlemen, will you also rise and raise your right hands and I will administer the oath. Do you swear that the testimony you are about to give is the truth, the whole truth, and nothing but the truth?

[Witnesses respond in the affirmative.]

Chairwoman MORELLA. Again, the record will show an affirmative response.

What we traditionally do is allow about 5 minutes for any opening statement that you may have, recognizing the fact that any written statement you have given us in its entirety will be included in the record.

So we will then start off with, if you have no particular preference, Mr. Scher.

TESTIMONY OF BARRY S. SCHER, VICE PRESIDENT, GIANT FOOD, INC., WASHINGTON, D.C.; J. PATRICK CAMPBELL, CHIEF OPERATING OFFICER AND EXECUTIVE VICE PRESIDENT, THE NASDAQ-AMEX MARKET GROUP, INC.; AND RONALD MARGOLIS, CHIEF INFORMATION OFFICER, UNIVERSITY OF NEW MEXICO HOSPITAL, HEALTH SCIENCES CENTER, REPRESENTING THE AMERICAN HOSPITALS ASSOCIATION

TESTIMONY OF BARRY S. SCHER

Mr. SCHER. Thank you very much. My name is Barry Scher and I am vice president for Giant Food. We operate 175 stores in Virginia, Maryland, the District of Columbia, New Jersey, and in Delaware. We are also a part of the Royal Ahold family——

Chairwoman MORELLA. Mr. Scher, I think that we had already said that Mr. Campbell would go first. I was simply looking at the manner in which we were seated.

Would you prefer to go first, Mr. Campbell?

Mr. CAMPBELL. No. Let him go.

Mr. SCHER. Either way.

Chairwoman MORELLA. Thank you very much. He is a good friend; he understands. Thank you.

Mr. SCHER. Giant is a part of the Royal Ahold family, a Netherlands-based international food retailer. In the United States alone, Ahold owns, aside from Giant Food, Stop & Shop based in Boston; Tops based in Buffalo; BI–LO from Maulden, South Carolina; and Giant Food Stores in Carlisle, Pennsylvania.

Our preparations for Y2K at Giant have been going on since 1996. We have been checking our numerous systems, one-by-one, to certify them as Y2K compliant. Although our administrative tests have given us a very high level of assurance that we will enter Y2K without system failures, our certifications test could not test how the systems would work together, as they do every day at Giant, when we enter the new year.

These early Y2K certifications were performed on system environments that were virtually identical to those that we use every day.

In August, these Y2K workhorses took on a new role at Giant. We ran our systems in a computer lab that simulated all the computer systems in a real store environment. There, our team moved

the test systems' clocks to December 31st. As the minutes and hour ticked away, the systems were used and monitored as they would be in a real store to see how they would operate as we entered the new year. We also wanted to see how they would handle the leap year day, February 29, 2000.

In the lab, everything worked just fine. We could place orders, ship, select, receive, weigh, and scan product, keep track of everyone's time and attendance, process prescriptions, and so on. Yet, there still loomed a larger question: Would all of these systems—stores, security, non-store environments—work together when the clock struck midnight and the new millennium began?

We decided that what we needed at Giant was a fully integrated test, doing exactly what we did in the lab; that is, advance the clock to the end of the year in an actual working store, while all of the systems were being used. Our concern was the potential impact that we would have on our business and the inconvenience to our customers if we field tested as customers shopped. Then, as so often happens, out of adversity, opportunity knocked.

In early September, we closed a store in Valley Forge, Pennsylvania. With no buyers available, the store was vacated and all the remaining product was shipped to a neighboring store. But before tearing out the computer systems and scales, our Y2K team was able to utilize this empty, but fully operational store to test our company's IT systems.

On September 28th, Giant put the computer systems to the ultimate Y2K test. They all passed. All of them, from EBT to DSD to POS, and these are food industry terms meaning such things as electronic benefit transfer, direct store delivery, and POS, which is point of sale or the front-end checkouts. The whole alphabet passed with flying colors.

While we are very confident in our own IT systems, we realize that there is always a chance that something could go wrong on January 1, 2000. As a result, we have developed a very comprehensive set of Y2K contingency plans that have been distributed just today, as a matter of fact, to all of our store and non-store management associates.

Now, in anticipation of peaks in consumer demand for certain products, we are also developing specific merchandising plans that include buying and distribution strategies. The focus will be on spreading the expected increased demand across the next few months by offering exciting promotions for certain products prior to the holidays. And when the holidays arrive, Giant's support system will not go on vacation. An expanded team of support associates will be on hand at Landover, where we are headquartered, and others will be on-call to address any and all issues that might arise come January 1, 2000.

We have also developed an internal and external communications plan. Our objective has been to inform and educate a number of stakeholders about our Y2K readiness. Just to cite some of the examples of our educational and informational activities:

We have developed a Y2K brochure, you should have it in front of you, I will hold it up in the event you do not. This brochure was given to all of our stores and distributed free to our customers. We

have also been asked to send it to area schools and other institutions. We have done so.

We have also placed newspaper advertisements in the Washington Post and Baltimore Sun. This is a copy of one. This was also placed in other major weekly newspapers throughout our marketing area.

We also decided to send personal letters to business, civic, and government leaders to inform them about our Y2K readiness. And, finally, we addressed business and civic groups, as we were often requested to do.

Plus we have done a great deal more—all with the objective of informing our customers and the general public that at Giant Food we are ready for Y2K.

And I mentioned earlier, Mrs. Morella, that I am speaking on behalf of the Ahold companies. All of the other Ahold companies are also ready. We are a member of the Food Marketing Institute, which is an international association representing food retailers. They have also testified before Congress. The food industry is, indeed, ready. Thank you.

[The prepared statement of Mr. Scher follows:]

Testimony by Barry F. Scher, Vice President-Public Affairs
Giant Food Inc.
Washington, D.C.
Congressional Committee on Government Management
Information and Technology

November 4, 1999

Good afternoon. My name is Barry Scher and I am vice president of public affairs for Giant Food. We operate 175 stores in Virginia, Maryland, the District of Columbia, New Jersey and in Delaware. We are a part of Royal Ahold, a Netherlands-based international food retailer. In the United States, Ahold also owns Stop & Shop based in Boston; Tops based in Buffalo; BI-LO based in Maulden, South Carolina; and Giant Food Stores of Carlisle, Pennsylvania.

Our preparations for Y2K at Giant Food have been going on since 1996. We have been checking our numerous systems, one-by-one, to certify them as Y2K compliant. Although our administrative tests have given us a high level of assurance that we will enter Y2K without system failures, our certifications could not test how the systems would work together – as they do every day at Giant – when we enter the new year.

These early Y2K certifications were performed on system environments (both main frame and non-main frame) that were virtually identical to those we use everyday.

In August, these Y2K "workhorses" took on a new role. We ran our systems in a computer "lab" that simulated all the computer systems in a real store environment . There, our team moved the test systems' clocks to December 31. As the minutes and hours ticked away, the systems were used and monitored as they would be in a real store to see how they would operate as they entered the "new year." We also wanted to see how they would handle the leap year day, February 29, 2000. In the lab, everything worked! We could place orders, select, ship, receive, weigh and scan product, keep track of everyone's time and attendance, process prescription orders and so on. Yet, there still loomed a larger question: Would *all* of our systems...security, store, non-store, etc. ...work together when the clock struck midnight and the new millennium began?

What was needed was a fully integrated test, doing exactly what we did in our lab – advance the clock to the end of the year – in an actual, working store, while all of the systems were being used. The concern was the potential impact on our business and the inconvenience to our customers if we field tested as customers shopped. Then, as so often happens, out of adversity, opportunity knocked.

In early September, we permanently closed a store in Valley Forge, PA. With no buyer available, the store was vacated, and all the remaining product was shipped to neighboring stores. But before tearing out the computer systems and scales, our Y2K team was able to utilize this empty, but operational store, to fully test our company's IT systems.

On September 28, Giant put its computer systems to the ultimate Y2K test! They passed! All of them...from EBT to DSD to POS...the whole alphabet passed with flying colors.

While we're very confident in our IT systems, we realize that there is always a chance that something could go wrong on 1/1/2000. As a result, we have developed a comprehensive set of Y2K **contingency plans** that have been distributed to all store and non-store management associates.

In anticipation of peaks in consumer demand for certain products, we are also developing specific **merchandising plans** that include buying and distribution strategies. The focus will be on spreading the expected increased demand across the next few months by offering exciting promotions for certain products prior to the holiday season.

And when the holidays arrive, Giant's **support system** will not be on vacation. An expanded team of support associates will be on hand in Landover, and others will be on-call, to address any and all issues that may arise come January 1, 2000!

We have also developed an internal and external communications plan. Our objective has been to inform and educate a number of stakeholders about our Y2K readiness. Just to cite some of our numerous educational and information activities, we have:

- Developed a Y2K brochure for our customers (copies will be distributed)
- Placed newspapers advertisements (ad copy to be shown)
- Sent personal letters to business, civic, and political leaders to inform them about our Y2K readiness
- Addressed business and civic groups

Plus we have done much more – all with the objectives of informing our customers and the general public that at Giant, we are ready for Y2K!

BIOGRAPHY

BARRY F. SCHER
VICE PRESIDENT- PUBLIC AFFAIRS
GIANT FOOD INC.

Scher is currently Vice President of Public Affairs for Giant Food Inc., a 175 store retail food/pharmacy chain serving Delaware, New Jersey, Virginia, Maryland and the District of Columbia. As a teenager, his first job was working as a part-time staffer in the Company's former Richmond division. To gain career experience in his chosen field of public relations, he worked while attending college at the NBC affiliate WXEX-TV in Richmond and later for the Spectator Newspaper Group in Washington, D.C. Scher holds a B.S. degree in journalism from William and Mary College's Richmond campus and also holds a Masters Certificate in public affairs from American University, Washington, D.C.

After college, Scher joined Giant full-time in 1966 as a member of the Company's newly formed Public Relations Department. He has held successive positions as Public Information Specialist, Communications Manager and Director of Giant's Communications Department. In 1977, the department took on additional responsibilities of handling legislative affairs among the local, state and Federal governments and Scher was promoted to Director of Public Affairs. He was named vice president in 1987.

Today the Public Affairs Department is responsible for Giant's government relations, news media relations, philanthropic programs, community affairs and external communication programs.

Scher currently holds offices in the following organizations:

* Board member of Second Harvest, a national organization based in Chicago representing food banks throughout the United States
* Chairman of the Board of the Capital Area Food Bank
* Chairman of the District of Columbia Government Environmental Planning Commission
* Member of the Board and chairman of the Legislative Committee, Virginia Food Dealers Association
* Executive Board Member, Virginia Retail Merchants Association
* First Vice-Chairman, Maryland Retail Merchants Association
* Board member, Maryland Business Roundtable for Education
* Director, Montgomery County Public Schools, Educational Foundation, Inc.
* Member of the Board of Directors, New Jersey Food Council
* Member of the Food Marketing Institute's Government Affairs and Communications Division
* Executive Committee of the Board of Directors, Maryland Chamber of Commerce

-OVER-

* Board Member and past president of the Board of Trustees of the Treatment and Learning Centers (TLC) for Disabled Children and Adults
* Executive Board Member and past chairman of the Mid-Atlantic Food Dealers Association
* Member of the Board of Advisors, Gallaudet University
* Member of the Board of Directors, Virginia Food Dealers Association

Scher belongs to the following organizations:

* The National Press Club
* The Public Relations Society of America
* The Montgomery County Press Association
* The Prince George's County Public Relations Association

9/99

GIANT FOOD INC.

BARRY F. SCHER
VICE PRESIDENT
PUBLIC AFFAIRS

DEPT. 589
BOX 1804, WASHINGTON, D.C. 20013
(301) 341-4710
FAX (301) 618-4967

February 1, 2000

To whom it may concern:

This is to inform you that Giant Food Inc. and its subsidiaries does not receive funds from the Federal Government for any reason.

Sincerely,

Barry F. Scher

Chairwoman MORELLA. Thank you very much, Mr. Scher. I do think this is an excellent pamphlet. It is colorful, it is accessible, it is understandable. And I commend you for it.

I am now pleased to recognize Mr. J. Patrick Campbell, chief operating officer of the NASDAQ stock market. Thank you, Mr. Campbell.

TESTIMONY OF J. PATRICK CAMPBELL

Mr. CAMPBELL. Thank you, Madam Chair. I am pleased to be here.

The SEC, the National Association of Security Dealers, the securities industry associations, and other firms, exchanges, and utilities have been leading the way in an industry-wide effort to be Y2K ready. The NASD and each of its companies are prepared to transition successfully into the 21st century, along with the rest of the securities industry. We are confident that our business systems, infrastructure, vendors, contingency plans, and transition command centers are ready. Investors should know that we have invested heavily to ensure that we are ready for the year 2000. In fact, the U.S. Senate and the GAO has given our industry its highest rating for Y2K preparedness.

The NASD began in 1996 to ensure that the business systems of the NASD companies will transition to the year 2000 successfully. We believe that our capital markets in the United States, our national treasures, and their integrity is paramount.

The NASD has spent $55 million, dedicated more than 100 staff to the effort. The NASD's year 2000 program has remediated over 300 applications, 11 million lines of code in mainframe, mid-range, and desktop systems. The securities industry has treated the problem just as seriously and has spent billions of dollars to meet the challenges that it poses.

Our programs have been focused in three areas: The readiness of NASD internal and market systems, the readiness of our 5,600 member broker-dealers, and, as important as anything, keeping investors well informed.

The first aspect of the NASD's year 2000 program deals with its internal systems, especially its market systems. The NASDAQ stock market and the American Stock Exchange, as well as all the other exchanges, participated in a series of successful Year 2000 industry-wide tests conducted over four weeks in March and April of this year. These full-cycle tests simulated the securities transactions process for the dates of December 29, 30, and 31, 1999, and for January 3, 2000.

The NASD tested its services with other participants, all the way from our NASDAQ workstation terminals through our network into our data center and back, end-to-end. The systems executed more than 170,000 simulated transactions for nine different security products over the tested dates. After this rigorous testing, we are confident that there will be no serious disruptions in our services and our markets, and that investors will be protected.

In addition to systems testing, we have also made extensive contingency plans to ensure business as usual, and to protect our computing and communications systems as well as our physical facilities. As part of these efforts, the NASD has established corporate

and business line command centers that will operate from late December through the first week in January 2000. We will pre-position staff, resources strategically in each of these centers, as well as around the country, to ensure rapid, fast response to protect investors' interests. These centers will be linked to the SEC and other industry organizations.

A second major area of NASD focus has been on its broker-dealer members. In 1998, the Securities and Exchange Commission adopted a rule requiring all broker-dealers to report their readiness through two successive filings. We use this information to help our firms meet the Y2K challenge.

We have held over 90 educational workshops, coordinated with extensive update materials. A year 2000 help desk has responded to member questions, approaching 20,000 in the last 2 years. We also have allowed firms to post letters dealing with their readiness on our web site to assure their investors that they can keep their money and assets safe.

The third major area of NASD Y2K focus has been on investor education. A comprehensive investor education program has resulted in a coordinated campaign with all the major markets, the SEC, the Securities Industry Association, and the President's Council on Year 2000. This coordinated campaign has communicated the readiness of the industry, as well as practical tips for investors preparing their personal finances for the transition.

Examples of these effort include a year 2000 investor kit, which has been made available to the members of the committee, and is also posted on our world-wide web, as well as an open investor letter, that ran today, by coincidence, in the Wall Street Journal. We will continue to run these letters by all the markets in the country basically expressing our Y2K position. This open letter outlines the industry's preparations and repeats the advice to investors found in our investors kit.

We appreciate this opportunity to testify. And you should take comfort that we have since 1996 exercised I think our fiduciary responsibility to the Nation and the people who are investors in our capital markets. Thank you.

[The prepared statement of Mr. Campbell follows:]

Testimony

of

J. Patrick Campbell
Chief Operating Officer
The Nasdaq Stock Market
National Association of Securities Dealers, Inc.

before the
Subcommittee on Technology of the
House Science Committee
and the
Subcommittee on Government Management,
Information and Technology of the
House Committee on Government Reform
on

Y2K Myths and Realities

November 4, 1999

I am Pat Campbell, Chief Operating Officer of the Nasdaq Stock Market, a subsidiary of the National Association of Securities Dealers, Incorporated. The NASD would like to thank the Committee for this opportunity to testify on "Y2K Myths and Realities." The Committee's invitation letter indicates that the purpose of this hearing is to respond to any looming myths, fears, and concerns with the Year 2000 (Y2K) problem. We welcome this opportunity to state what we have done to address the Y2K problem and to allay any fears that investors in our market may still harbor. As a preliminary matter, I would also like to note for the record that the NASD has not received any federal funding in the last two fiscal years.

The NASD

Let me briefly outline the role of the NASD in the regulation and operation of our securities markets. Established under authority granted by the 1938 Maloney Act Amendments to the Securities Exchange Act of 1934, the NASD is the largest self-regulatory organization for the securities industry in the world. Virtually every broker-dealer in the U.S. that conducts a securities business with the public is required by law to be a member of the NASD. The NASD's membership comprises 5,600 securities firms that operate in excess of 75,000 branch offices and employ more than 600,000 registered securities professionals.

The NASD is the parent company of The Nasdaq Stock Market, Inc., the American Stock Exchange, and NASD Regulation, Inc. (NASDR). These wholly owned subsidiaries operate under the authority of the parent, which retains overall responsibility

for ensuring that the organization's statutory and self-regulatory functions and obligations are fulfilled. The NASD is governed by a 33-member Board of Governors, a majority of whom are non-securities industry affiliated. Board members are drawn from leaders of industry, academia, and the public. Among many other responsibilities, the Board, through a series of standing and select committees, monitors trends in the industry and promulgates rules, guidelines, and policies to protect investors and ensure market integrity.

NASD Regulation

NASD Regulation is responsible for the registration, education, testing, and examination of member firms and their employees. In addition, it oversees and regulates our members' market-making activities and trading practices in securities, including those that are listed on The Nasdaq Stock Market and those that are not listed on any exchange.

NASDR carries out its mandate from its Washington, D.C. headquarters and 14 district offices located in major cities throughout the country. Through close cooperation with federal and state authorities and other self-regulators, overlap and duplication is minimized, freeing governmental resources to focus on other areas of securities regulation.

NASDR has examination responsibilities for all of its 5,600 members. In addition to special cause investigations that address customer complaints and terminations of

brokers for regulatory reasons, NASDR conducts a comprehensive routine cycle examination program.

The American Stock Exchange

The American Stock Exchange is the nation's second largest floor-based securities exchange, listing 770 companies, and is the only U.S. securities exchange that is both a primary market for listed equity securities as well as a market for equity options, index options, and equity derivatives. Amex has been the primary innovator in structured derivative securities and index share securities.

The Nasdaq Stock Market

The Nasdaq Stock Market is the largest electronic, screen-based securities market in the world. It currently is capable of handling trading of up to four billion shares a day and can be scaled up, if necessary, to accommodate an eight billion share day. Founded in 1971, Nasdaq today accounts for more than one-half of all equity shares traded in the nation and, since January of this year, is also the largest stock market in the world in terms of dollar value of shares traded. Trading volume on Nasdaq in 1999 has routinely surpassed a billion shares per day, with a peak of 1.437 billion shares reached just last Friday, October 29, 1999. Nasdaq lists the securities of 5,288 domestic and foreign companies, more than all other U.S. stock markets combined. There are over 70 million investors in Nasdaq companies. The Nasdaq Stock Market is made up of two distinct

markets. the Nasdaq National Market and, for smaller companies, the Nasdaq SmallCap Market.

Securities Industry Readiness

The Securities and Exchange Commission (SEC), the Securities Industry Association (SIA), the NASD, and other firms, exchanges, and utilities have been leading the way in an industry-wide effort to be Y2K ready. The NASD and each of its companies are prepared to transition successfully into the 21st century, along with the rest of the securities industry. We are confident that our business systems, infrastructure (i.e., facilities, networks, etc.), vendors, contingency plans, and transition command centers are ready. Investors should know that we have invested heavily to ensure that we are ready for the Year 2000. In fact, the U.S. Senate has given our industry its highest rating for Y2K preparedness.

In March and April of this year, the securities industry's computer systems for order processing, trade execution, settlement and clearing were checked, tested, and re-checked. Securities firms, data vendors, exchanges, and utilities all collaborated in one of the largest, most complex tests of computer systems ever undertaken by the industry. Nevertheless, many teams of specially trained personnel will be closely monitoring the securities markets to make the transition to the new year as seamless as possible. Because of the seriousness of the potential problem, there is no such thing as being over-prepared.

With this said, we do believe that there will be Year 2000 "events" that could occur. These will fall into several categories: (a) minor problems that will be of no

significant business concern (i.e., "oops"), (b) minor problems that will be of a business concern (e.g., a problem in one data source; however, the data is available from another data source), (c) problems that will slow down a business process but not be visible to the public, and (d) Y2K problems that will affect business processing and will be visible to the public. We are confident that there will be a minimum number of items in the last category in the financial services industry.

The NASD Year 2000 Program

The NASD implemented a comprehensive Year 2000 Program in 1996 to ensure that the business systems of the NASD companies will transition to the Year 2000 successfully. The program has focused on the readiness of NASD internal systems, the readiness of our 5,600 member broker-dealers, and keeping investors informed about the industry's preparedness efforts. It is critical to the stability of the markets to do everything we can to instill confidence in investors – confidence that when trading begins on January 3, 2000, their investments will be both safe and accessible.

This NASD commitment has resulted in spending of $55 million, and the dedication of more than 100 staff during our efforts to address the Year 2000 challenges. The securities industry has treated the problem just as seriously, and spent in the billions of dollars to meet the challenges it poses.

In the NASD's Year 2000 Program over 300 applications and 11 million lines of code in mainframe, mid-range, and desktop systems have been remediated. Over the last three years, our oversight has included extensive audits of the program's management and results by internal and external organizations.

Our efforts have been focused on our markets, our member firms, and investors.

Nasdaq Amex Market Preparedness

The Nasdaq Stock Market and the American Stock Exchange participated in a series of successful Year 2000 industry-wide tests conducted in March and April 1999. This testing enabled us to determine whether our vast array of sophisticated computer systems could process equities transactions in the Year 2000. These full-cycle tests simulated the securities transaction process, from customer order input, through the markets' systems, and finally to settlement at the National Securities Clearing Corporation. Over a period of four weekends, the dates December 29, 30, 31 of 1999 and January 3, 2000 were simulated with transactions processed by all major participants in the securities industry. Through the tests with these date changes, the NASD tested its services with other participants, from our Nasdaq Workstation terminals through our MCI WorldCom network (the second largest private network in the United States), into our data center and back. Over 160 employees contributed to the testing of Nasdaq/Amex's major trading systems for equities and options. The systems executed more than 170,000 simulated transactions for nine securities products for the tested dates. After this extensive, rigorous testing, we are confident that there will be no serious disruptions in our services—and that investors will be protected.

Additionally, in order to ensure "business as usual," Business Continuity Plans have been created to provide further protection for our computing systems, physical facilities, and communications systems in case of unexpected events. The NASD Business Continuity Planning program provides the structure to ensure continuity of critical business functions. As part of these preparedness efforts, the NASD has established a corporate Coordination and Communications Center and business line

Response Centers that will be in operation from late December through the first week in January 2000. Communications and facilities will be ready to respond to problems that may occur during the transition weekend. We will pre-position staff and resources strategically in our corporate command center, and in each company response center. In addition, we will pre-position staff around the country to ensure fast response to protect investors' interests. Direct communications links will be established with the SEC and other industry organizations. Planning for major scenarios has been completed jointly by the SEC, SIA, major markets, exchanges, and Self Regulatory Organizations (SROs).

During the transition period, investors could lose confidence by misinterpreting events, and any incident will likely be perceived to be Y2K related. The NASD will therefore quickly report on any problems, their causes, and the impact they may have.

From an industry-wide perspective, the SEC is leading an effort that includes the implementation of structured information data collection centers that are tied together with assured communications to facilitate "business as usual" decision-making. All major industry organizations and governmental agencies will be coordinated through communications and reporting systems. This industry's current consensus management approach, which includes all major elements of the industry, will be used to manage such events. Planning for major scenarios has been completed jointly by the SEC, SIA, major markets, exchanges, and SROs.

The NASD Broker-dealer Membership Program

The initiative of readying member firms for the new century transition began more than three years ago and has been one of the most important, all-encompassing initiatives undertaken by the NASD. This effort benefits not only investors, but all

NASD member firms, by providing the guidance needed to help firms complete their own readiness efforts. The following describes the range of activities that the NASD has undertaken to support the industry and its member firms.

In 1998, the SEC adopted a rule requiring all broker-dealers to report their readiness through two successive Form BD-Y2K filings. This all-inclusive reporting approach provided securities regulators with information to assess industry readiness and to assist securities firms in achieving readiness. Prior to this reporting rule requirement, the NASD had implemented a member firm readiness assessment survey to determine where the focus of our membership was relative to their Year 2000 initiatives.

Using the individualized information provided by our members through their BD-Y2K filings, the NASD dedicated substantial resources to assist all firms with their preparation, especially our smaller firms. Over 90 educational readiness workshops and seminars were held, coordinated with update materials that included brochures, letters, electronic messages, Web pages, and telephone communications.

Early in the process, the NASD established a Year 2000 Help Desk to respond to member questions and concerns. In addition, a team of Year 2000 readiness analysts trained in measures specific to the securities industry has been monitoring the progress of NASD members while focussing firms on their Year 2000 efforts. During 1998 and 1999, NASD analysts and the Help Desk communicated on these efforts more than 20,000 times with member firms through telephone calls, e-mails, faxes, and letters.

To assist firms further in communicating their readiness efforts to their investors, we also implemented a voluntary Member Year 2000 Readiness Program to allow members to display a Year 2000 readiness letter or statement on the NASD and NASDR

Web Sites. These letters assure the investing public of their broker-dealers' ability to handle Year 2000 problems and keep their money and assets safe.

Investor Education and Communication

Through continuous contact with member firms, analysis of national survey data, and information provided by the SEC, SIA, and others, we have been able to assess investor confidence levels related to the Year 2000 to guide our overall investor communications program.

Our comprehensive investor education program has resulted in a coordinated campaign with major markets, exchanges, the SEC, the SIA, and the President's Council on Year 2000 Conversion. This coordinated campaign has communicated the readiness of the industry, as well as practical tips for investors for preparing their personal finances for the transition. In September 1999, these organizations, in addition to the New York Stock Exchange (NYSE), joined to outline the extensive steps undertaken by Wall Street, the mutual fund industry, and regulators to ensure that it will be "business as usual" when the Year 2000 arrives.

To educate investors further, the President's Council, SEC, SIA, NASD, and the Investment Company Institute developed a "Year 2000 Investor Kit." The kit helps investors prepare for the Year 2000 and includes tips such as:

- Keep good records (an idea that makes good sense at any time);
- Stay informed about what their financial service providers are doing to become Y2K ready;
- Get Y2K literature provided by their broker-dealers, mutual funds, investment advisers or public companies in which they hold;

- Invest for the long term and avoid changing trading habits;
- Do not worry about obtaining stock certificates; and
- Check the Y2K readiness of personal computers.

The kit also features a review of industry efforts to prevent Y2K computer problems, a list of frequently asked questions for investors, a Year 2000 checklist, and information on how to check personal computers and fax machines for Y2K problems. In addition, the kit cautions investors about fraud and includes the following tips:

- Do not listen to, or respond to fear, uncertainty, and doubt caused by unsubstantiated rumors;
- Be on the lookout for fraud, since some people may will try to capitalize on these fears about the Y2K problem; and
- Be careful if someone tries to sell you a product, service, or investment that is "guaranteed" to fix or prevent a Year 2000 problem.

The public can access the Year 2000 Investor Kit through the NASD Web site: http://www.nasdr.com/3600_inv_kit.htm. Printed copies are available by calling 1-888-227-1330 or sending an email to y2k@nasd.com. The kits have also been provided to securities firms for distribution to their clients.

In addition, investors can check on the Y2K preparedness of broker-dealers, mutual funds, and investment advisors on the SEC Web site at: http://www.sec.gov/news/y2k/y2kreps.htm.

Working together, the SIA, the NASD, the NYSE, the Depository Trust & Clearing Corporation, the Boston Stock Exchange, the Chicago Board Options Exchange, the Chicago Stock Exchange, the Pacific Exchange, and the Philadelphia Stock Exchange

61-629 00 - 5

have expanded the industry's extensive public education campaign on how the industry has addressed the Year 2000 problem. The latest effort in the industry's program to separate Y2K fact from fiction is an open letter to investors that will run as an advertisement in major daily newspapers in the next few weeks, including the *New York Times*, the *Wall Street Journal*, the *Washington Post*, and the *Los Angeles Times*. This open letter outlines the industry's Y2K preparations and repeats the common sense advice to investors found in the industry's Year 2000 Investor Kit on how to get ready for Year 2000. The letter advises the following:

- Stay the Course. Is there anything you should be doing as Y2K approaches? Yes. Keep in mind a few practical guidelines that we encourage you to follow – Y2K or not.
- Stay invested for the long term. We believe the market will continue to reward prudent investors with the patience to stick to sound investments over time.
- Continue keeping good records. Review and save your account statements, confirmation slips, and other financial information.
- Leave stock certificates in the safekeeping of your securities firms. There is no need to risk their loss by needlessly moving them.
- Learn the facts. If you have concerns, talk to a representative of the firm serving you and learn more about its Y2K safeguards.

The industry plans to follow-up on the Y2K campaign with an Internet communications program that will make industry experts available for on-line chats with investors.

Conclusion

Summarizing the NASD's efforts, Frank Zarb, Chairman and CEO of NASD said

> "A top priority over the past several years has been to educate the 5,000-plus member-firms of the National Association of Securities Dealers about the importance of Year 2000 readiness, and we have monitored our membership closely to ensure compliance...we've also worked hard to make sure that the internal systems of the Nasdaq Stock Market and American Stock Exchange are up to the challenge of the Year 2000 transition, and that we have communicated our readiness to investors. We feel confident that the integrity of our markets will be preserved and the investor will be protected."

Thank you for this opportunity to testify on this important issue. I would be happy to answer any questions you may have.

J. Patrick Campbell
Chief Operating Officer and Executive Vice President
The Nasdaq-Amex Market Group, Inc.

J. Patrick Campbell joined the National Association of Securities Dealers, Inc. (NASD®), in January 1997 in the newly created senior management position of Executive Vice President, Market Services. In his current position, Campbell is responsible for the day-to-day operation of The Nasdaq Stock Market®, the American Stock Exchange®, and all other market services offered by both. He helps ensure that both marketplaces are clearly focused on meeting the needs of members, issuers, and the investing public—both domestically and internationally.

Prior to joining the NASD, Campbell was Senior Executive Vice President of The Ohio Company, where he was responsible for equity trading, research, portfolio management, and retirement plans administration. He was also a member of the firm's Board of Directors and Executive Committee. While a senior executive for The Ohio Company, Campbell was a member of the Nasdaq Board of Directors (1990-1993) and a member of the Cincinnati Stock Exchange (1980-1985).

Campbell is a graduate of Ohio University (1971) and completed SIA's Securities Industry Institute-Wharton School of Finance (1979). He and his wife, Ellen, have two children.

current as of: 04/22/99

Chairwoman MORELLA. Thank you, Mr. Campbell, for your testimony and for what has been done. And thank you for being such a great constituent.

Mr. CAMPBELL. Thank you.

Chairwoman MORELLA. I am now pleased to recognize Mr. Ronald Margolis, chief information officer at the University of New Mexico Hospital in Albuquerque, and also representing the American Hospital Association.

Mr. Margolis.

TESTIMONY OF RONALD MARGOLIS

Mr. MARGOLIS. Thank you, Madam Chair. I am Ron Margolis, chief information officer at University of New Mexico Hospital in Albuquerque. I am here on behalf of the American Hospital Association and their 5,000 hospitals, health systems, networks, and other providers.

I would like to focus on four questions about year 2000 and hospitals: Will hospitals be ready? How have hospitals been preparing over the past few years? What if something goes wrong? Finally, how are hospitals reassuring the public at this last 55 days?

Will hospitals be ready? In a word, the answer is, yes. An AHA survey last spring found that 95 percent of hospitals expected that their medical devices, computerized information systems, and infrastructure to be Y2K compliant or to operate without a problem on December 31st. A report issued last month by the Health and Human Services Office of Inspector General also indicated high confidence in hospitals' Y2K readiness.

For example, in New Mexico, our State Hospital Association survey very recently found that all systems directly related to patient care were expected to be compliant by the year's end, and right now are greater than 96 percent prepared. It is reasonable to infer that since these surveys were conducted earlier in this fall season, readiness among all hospitals has increased.

How are hospitals preparing? Hospitals have taken inventory of all of our equipments—that's medical devices, computer systems, hardware and software. From that inventory, a remediation or repair plan was developed and is now being completed. We have tested, using rigorous means, all of our computer systems with a special priority toward patient care systems to ensure that they will work well into the next millennium. We have developed and acquired software that allows us to warp the time ahead so that we were able during the summer to test systems for the period December 27th through April 1st, which includes the leap year which is unusual this next year as well as January 1st.

Also, through manufacture and vendor contact, we have determined other systems in medical devices which may be affected and how they will be affected. We are following up as required, which could mean anything from repairing a device, loading new software, or taking a device out of service for the period of the date change.

Also, all hospitals plan to increase the level of staffing during the days surrounding the millennium date change. Hospital personnel will be on hand during the date change to make sure equipment is safe and working properly before being used on any patients.

Let me point out that hospitals are somewhat unique in their use of technology. It is used as a clinical efficiency aide. Clinicians, of course, are fully able to perform nearly every function that patient support devices provide. We do not under any circumstances hook patients up to computers and then ignore their humanness; we certainly will not on December 31st. To paraphrase the slogan of a telephone company: In the medical world of technology, people make a difference, and we truly believe that is a major differentiator.

Nationally, the American Hospital Association is working with the President's Council on Y2K Conversion and with other associations to make sure the availability of drug products, pharmaceuticals, and medical supplies will continue as needed into the new year. In New Mexico, hospitals are working closely with the two major drug houses to assure uninterrupted distribution of pharmaceutical supplies.

What if something goes wrong? Here in Washington, members of the District of Columbia Hospital Associations have pledged to back each other up in case of any kind of trouble or high demand for patient services. A Memorandum of Understanding provides a blueprint for inter-hospital support. This kind of cooperation is happening in communities all across America.

In my State, hospitals are sharing information on medical devices, contingency plans, and performing readiness drills. We have emergency preparedness procedures in place at the State, county, and the local levels. We have emergency power generation capabilities that support all of our critical care and emergency care facilities.

Finally, how are hospitals reassuring the public? As hospitals continue to perform their inside preparations, they are also reaching out to the communities. They are holding town meetings to ensure the people they serve are aware of what is being done. For example, New Mexico hospitals are taking part in Y2K community conversations. In Albuquerque, local hospitals are participating in the Mayor's Millennium Committee which has provided a public forum for citizens' concern and input.

In summary, the AHA distributed to all of its members "Health Care and Y2K: What You Need to Know About Health Care and the Year 2000." This booklet was developed jointly by the President's Council with the help of the American Hospital Association and other affiliated organizations to focus on consumer questions about Y2K. We encouraged all our members to make this easy to read booklet available to their communities.

To conclude, Madam Chairperson, the year 2000 issue will affect every aspect of American life, but few, if any, are as important as health care. What I have outlined today is merely a snapshot of a much more in depth and thorough and united effort to ensure patient safety at midnight on January 1st and beyond. Hospitals and health care systems, their State associations, and the AHA are working together toward a smooth and healthy transition into the new millennium. Thank you.

[The prepared statement of Mr. Margolis follows:]

I will focus on four key questions: Will hospitals be ready? How are hospitals preparing? What if something goes wrong? And, finally, How are hospitals reassuring the public?

WILL HOSPITALS BE READY?

The majority of America's hospitals expect to be completely "Y2K compliant" by January 1, 2000. Based on the results of a nationally representative survey that the AHA conducted, almost all of the remainder expect to be sufficiently prepared that critical operations will not be affected. At the time the survey was conducted last Spring, more than 95 percent of hospitals expected their medical devices, information systems, and infrastructure – such as elevators and electrical systems – to be Y2K compliant by year end or expected no problems in their operations.

In the survey, hospitals were asked whether their medical devices would be compliant, or non-compliant with no adverse effects. This is important, because some medical devices could technically be labeled non-compliant, even though they will operate – and do so safely – during and after the date change.

For example, an EKG machine may provide accurate heart rate information, while the strip recording the test information notes the date of the test incorrectly. In such cases, medical personnel would simply write the correct date onto the readout. In no way would this machine be a danger, but it technically would be labeled non-compliant because it did not recognize the date change.

I will focus on four key questions: Will hospitals be ready? How are hospitals preparing? What if something goes wrong? And, finally, How are hospitals reassuring the public?

WILL HOSPITALS BE READY?

The majority of America's hospitals expect to be completely "Y2K compliant" by January 1, 2000. Based on the results of a nationally representative survey that the AHA conducted, almost all of the remainder expect to be sufficiently prepared that critical operations will not be affected. At the time the survey was conducted last Spring, more than 95 percent of hospitals expected their medical devices, information systems, and infrastructure – such as elevators and electrical systems – to be Y2K compliant by year end or expected no problems in their operations.

In the survey, hospitals were asked whether their medical devices would be compliant, or non-compliant with no adverse effects. This is important, because some medical devices could technically be labeled non-compliant, even though they will operate – and do so safely – during and after the date change.

For example, an EKG machine may provide accurate heart rate information, while the strip recording the test information notes the date of the test incorrectly. In such cases, medical personnel would simply write the correct date onto the readout. In no way would this machine be a danger, but it technically would be labeled non-compliant because it did not recognize the date change.

More recently, a report issued last month by the Health and Human Services' Office of Inspector General (OIG) also indicates high confidence in hospital Y2K readiness. The OIG report reaffirms what we've been hearing from our hospitals on their Y2K efforts: that Y2K is a critical issue which they are actively working to address because their number one priority – as always – is patient safety. The fact that hospitals represented the largest percentage of responses to the OIG report shows their willingness to be forthcoming about their Y2K preparation.

The Healthcare Year 2000 Readiness Assessment #2, prepared for the Health Care Financing Administration (HCFA) by the Rx2000 Solutions Institute and released earlier this year, identified hospitals as the healthcare sector that is "among the most aggressive towards meeting its Year 2000 deadlines."

In New Mexico, the state hospital association surveyed select hospitals across the state in May and June. The survey group was representative of New Mexico's patient population and geographic dispersion. The survey found that, in May and June:

- All systems directly related to patient care were expected to be compliant by year-end.
- Most contingency and disaster recovery plans were written and ready to go, with the rest to be complete by this fall.
- More than half of physical plant systems were ready, with the rest moving towards readiness without difficulty.
- Every respondent was involved with community and supply chain discussions. All have been in contact with their local public safety departments, county and city governments,

utilities, the local and regional blood banks, pharmaceutical suppliers, medical waste contractors, and home care agencies to discuss readiness and share operational issues.

With the amount of time that has passed since the New Mexico survey, as well as the AHA and OIG surveys, it is reasonable to infer that readiness status among all hospitals has improved and increased. Taken together, all of these – the AHA survey, the OIG survey, the Rx2000 survey, and my state's survey – point toward the same conclusion: hospitals expect to be ready to meet the Y2K challenge.

HOW ARE HOSPITALS PREPARING?

America's hospitals and health systems are working very hard to prepare all aspects of their operations for the date change: devices and equipment, information systems, and infrastructure. For example, hospitals have been taking the following steps to ensure the safety and reliability of their services at the turn of the century:

- Taking inventory of all equipment and devices and support systems – identifying which may be potentially affected by Y2K.
- Determining which are actually affected and how their functioning will be altered – this is done through contact with the manufacturers and vendors to get the results of their assessments and testing.
- Taking follow-up action if those devices or equipment are affected by Y2K – depending on the device or equipment, this may mean repairing, taking out of service, or training staff on how to use the equipment going into the new year.

- Developing contingency plans – even with all the advance preparations, hospitals still need to anticipate the unforeseen.

To ensure the readiness of medical devices, the AHA, the Food and Drug Administration (FDA) and the manufacturers and their representatives have been collaborating to ensure that the FDA's Federal Year 2000 Biomedical Equipment Clearinghouse is receiving accurate and useful information that in turn is useful for hospitals. This information is easily available on the agency's Web site at www.fda.gov.

It is also important that the FDA play a proactive "rumor control" role, monitoring such arenas as the Internet and the media to make sure that information that circulates about the effects of Y2K on medical devices and equipment is accurate, and correcting it when it is wrong.

The AHA also is working with the President's Council on Year 2000 Conversion, as well as with other associations and sectors of the health care field, to make sure the availability of drugs, pharmaceuticals and medical supplies will continue as needed into the new year. The exchange of information between hospitals and their suppliers, as well as joint contingency planning, are essential steps to avoid the hoarding or stockpiling that would lead to shortages.

The AHA is focusing on a broad range of other suppliers to get the vendor information our members need, from medical device manufacturers to pharmaceutical and other medical supply companies. Experts in the field are advising health care organizations to employ a risk management methodology to identify their most critical supply issues, focusing on those that are

critical to patient health. Hospitals must know how their suppliers and manufacturers plan to deal with potential disruptions to the flow of medical and surgical supplies, or the raw materials necessary to produce those supplies.

The AHA recently sent a Y2K Advisory to every AHA member, also available on our Web site, detailing how hospitals can put together a responsible course of action in the face of stockpiling concerns. In the advisory we advised hospitals that stockpiling and hoarding can cause the very shortages that they should be trying to avoid. We also used the advisory to urge hospitals to agree to act as each other's backup in case of Y2K-related difficulties.

WHAT IF SOMETHING GOES WRONG?

Right here in Washington, DC, for example, members of the District of Columbia Hospital Association (DCHA) have pledged to back each other up in case of trouble. In order to support each other in case of a Y2K emergency, district hospitals are linked to each other through the Hospital Mutual Aid Radio System. And a Memorandum of Understanding (MOU) is in place that provides a blueprint for inter-hospital support.

Both the radio system and the MOU address communications during disasters for appropriate care of patients, sharing of staff, and dispensing of equipment and pharmaceuticals. DCHA's Y2K committee has been consolidating other efforts by monitoring Y2K reports for common outside vendors that may have an impact, such as utilities, financial institutions, and the local government.

This kind of cooperation is happening in communities all across America. The reason is simple: Hospital care is not provided in a vacuum. It requires the help of utilities such as electricity and water; it requires emergency services such as police and fire departments; it requires cooperation with other health care providers; it requires partnership with local governments; the list goes on. To ensure that these requirements are not interrupted, many hospitals are working with other local health care providers, local agencies, police and fire departments.

Another example is a recent drill in California. Three hundred and seventy two hospitals took part. The drill tested the statewide coordination of communications systems, the transmission of data about available hospital beds, and the hospitals' own contingency plans for Y2K. All tests were completed successfully.

In Hartford, Connecticut, last month, local emergency services personnel and three hospitals participated in the city's Y2K readiness drill, complete with a fake bus collision, injured volunteer children, and power outages. The drill went smoothly.

In New Mexico, hospitals have been working with each other and sharing information on medical devices, laboratory contractors, contingency plans and readiness drills throughout this entire Y2K preparation process. New Mexico hospitals are preparing for contingencies by making sure staff levels will be higher than normal across the state at the turn of the clock, with staff on-site or on-call and available within 30 minutes of a page. Local hospitals also have been working with regional emergency medical services personnel to staff, monitor and coordinate Emergency Command Centers in case rapid response is needed for medical emergencies.

On a national level, the AHA is working with the President's Council on Year 2000 Conversion on the Year 2000 Information Coordination Center, which was created in June. Information available from the center can serve as an early warning system, enabling hospitals and other providers to manage their resources and responses better than if they try to handle things alone.

America's hospitals and health systems are in the business of dealing with the unexpected. They are used to mobilizing quickly in the face of floods, hurricanes and potentially disastrous events that are an unfortunate fact of life. Because patient safety is the highest priority for hospitals and health systems, our ultimate contingency plan is to take care of patients at the bedside – as we do 24 hours a day, seven days a week, 365 days a year.

Contingency planning is not being done out of a sense of panic, but to provide the broadest latitude for dealing with the unexpected. Some devices and equipment can only be operated in real-time – that is, after the clock turns from Dec. 31 to Jan. 1 – and hospital personnel will literally watch this equipment's clock change to ensure that it works properly before allowing it to be used for patient care. The ultimate contingency plan is to provide care the old-fashioned way in the unlikely case of a modern medical device impeding care.

HOW ARE HOSPITALS REASSURING THE PUBLIC?

Hospitals and health systems face the same kinds of Y2K concerns as other critical sectors of our nation. However, hospitals are unique. They have a special place in America's social services safety net. Every community in America relies on its local hospital to be ready to provide high-quality health care services on demand, 24 hours a day. It is therefore very important that the

public understand that hospitals have been very aggressive in their efforts to ensure the seamless delivery of health care services before, during, and after the turn of the century.

So, as hospitals continue to perform their "inside" preparations, they also are reaching out. Hospitals are deeply involved in efforts to communicate with their communities about the conversion to the Year 2000. For example, the AHA helped sponsor one of the White House Community Conversations, in St. Louis. And we have encouraged every hospital to get involved when the Community Conversations come to their towns.

The AHA also distributed to all its members "Health Care and Y2K: What You Need to Know About Health Care and Year 2000." This booklet was developed to address many of the questions consumers have about the Y2K issue and its possible impact on health care. It also provides consumers with important suggestions about what they can do for themselves and their loved ones to plan responsibly for the Year 2000 date change. We encouraged all our members to make this easy-to-read booklet available to their communities.

The AHA, in collaboration with our state, regional and metropolitan associations and other key strategic partners, is working hard to stress to our member hospitals the importance of managing the Y2K issue from a public confidence perspective. We have developed tools to counsel hospitals and health systems about how to talk with the public about Y2K and health care. A Y2K Communications Action Kit was distributed to our members, who adapted the materials in the kits for use in their communities.

A four-page insert will be included next week in *AHA News*, our national newspaper, guiding hospitals through the final 50 days of 1999, with emphasis on community confidence. This comes on the heels of many other articles on Y2K, plus a regular column of information and advice. Several other national publications published by various AHA membership societies also have been focusing heavily on Y2K issues. Several of these societies, such as the American Society for Healthcare Engineering, the American Society for Healthcare Risk Management, and the Association for Healthcare Resource and Materials Management, are helping their members attack the millennium bug in their hospitals.

In New Mexico, hospitals are also taking steps to answer the public's questions, including participating in local Y2K Community Conversations. And hospitals in my city have been participants in the Mayor of Albuquerque's "Millennium Committee."

CONCLUSION

Mr. Chairman, the Year 2000 issue will affect every aspect of American life, but few, if any, are as important as health care. America's hospitals and health systems, their state associations, and the AHA are partners in the effort to prepare for the Year 2000. Together, we are working to ensure a smooth – and healthy – transition into the new millennium.

THE UNIVERSITY OF NEW MEXICO · HEALTH SCIENCES CENTER
UNIVERSITY HOSPITAL

Ronald B. Margolis

Ronald Margolis is the Chief Information Officer of the University of New Mexico Hospital in Albuquerque, NM, a position he has held for two and a half years. In this position, he is responsible for all computer information systems, telecommunications systems, and computer-based medical devices. The University of New Mexico Hospital is the only teaching hospital and Trauma I center in the substantially rural state of New Mexico.

Mr. Margolis has been in healthcare systems management for over 18 years, holding technical and management positions, with organizations such as Arthur D. Little, Harvard Medical School and the Massachusetts Hospital Association. He has served on technology advisory committees in the New Mexico State Hospital Association and the University Hospitals Consortium.

Mr. Margolis holds a BA degree from the University of Texas and a MBA in Computer Science from the University of Missouri.

2211 Lomas Blvd. N.E. • Albuquerque, New Mexico 87106 • (505) 272-2111

Chairwoman MORELLA. Thank you, Mr. Margolis.

I am going to turn for questioning now first to a gentleman who has not had a chance to ask questions, the distinguished Ranking Member of the Government Management, Information, and Technology Subcommittee of the Government Reform Committee, Mr. Turner, the gentleman from Texas.

Mr. TURNER. Thank you, Mrs. Morella.

I want to commend each of our three witnesses on this panel. I can tell you have invested many hours and many dollars in trying to be ready for Y2K. I have always held the opinion, at least after our many months of study on this committee, that it is the myths about Y2K that could hurt us rather than the realities.

I did not get the chance to ask Mr. Koskinen a question that I really think I will direct at Mr. Willemssen. He in his work with the GAO probably knows the answer as well as Mr. Koskinen. The Council that Mr. Koskinen has an Information Coordination Center which, as I understand it, is designed to be a place that is kind of a central point for coordinating all information about Y2K problems, about events that surround the new year.

It seems to me that our emphasis at this point, after months of preparation, which I feel very good about, both in the public and the private sector, that we need to rethink a little bit about what we are doing to prepare to address the rumors and the myths that may surround the New Year. At one of our recent meetings, I even suggested that perhaps Mr. Koskinen's council should bring aboard some high profile, credible personality to be a spokesperson, someone who could answer press inquires and someone who could pass along the realities and dispel the myths, someone of the caliber of Walter Cronkite.

But it seems to me that is our real fear. I can sense, Mr. Campbell, that you and the securities market would be particularly sensitive to the rumors and the myths that may float around the new year. I come from a small town and in a small town we used to all understand that there were a lot of rumors that started at the bridge clubs and at the coffee shops, and if you circulated in the right groups you could pick up on those rumors, and they would pretty quickly get around town.

With the advent of mass media, television, radio, obviously, information spreads much faster all across the country. But at least there, there is responsible journalism to kind of screen the information that comes across the airwaves. But on the Internet, you can put anything on there you want to and spread that story to tens of thousands of people in a matter of hours. Most of us on this committee have experienced in our own offices receiving large volumes of mail on subjects that our constituents heard about over the Internet that we turn around and have to write letters back to them and tell them what they read is absolutely false, there is no such proposal in Congress to tax the Internet, or whatever the issue happens to be.

And I am fearful that Y2K offers the opportunity for pranksters and for outright frauds to run rampant on the Internet, and that we need to be very careful about how we structure Mr. Koskinen's Information Coordination Center to be sure that it is going to not

only be able to process all of the myths that may surround the new year, but be able to speak with credibility to dispel those myths.

Mr. Willemssen, do you know what Mr. Koskinen has done to ensure that we are going to have that kind of response in place?

Mr. WILLEMSSEN. I was over at the Information Coordination Center on Monday. They are located on about 18th and G. We got a tour, my staff did, of the facility. They do have a press briefing room set up I think for about 60 people. And as I recall, General Kind, the head of the ICC, mentioned to me that the plan was for Mr. Koskinen to provide press briefings approximately every 4 hours during that rollover period.

Secondly, echoing back to one of the comments you made earlier, as one of the ideas that we have suggested before, especially now that we are in November and entering into December, is the executive branch may want to look at opportunities to use public service announcements now and in December rather than waiting for just the rollover period, especially to the extent that some may start to view Y2K as entertainment opportunities, as opportunities to show worst case scenarios. I think given that, it is best to combat those kinds of announcements with facts, the facts that we have discussed here today. So I think there still is an opportunity prior to that rollover period to come out with those kind of announcements.

Mr. TURNER. Mr. Campbell, do you have similar plans for the securities industry to be able to speak with credibility to dispel rumors?

Mr. CAMPBELL. Congressman Turner, yes, we do. We expect fully to have our command centers staffed from the 28th of December on. We have hot links, hot lines, satellite communication, et. cetera, with our vendors, with the news media, with the President's working group, with the Securities and Exchange Commission. We have a broadcast facility at which we expect to have Frank Zarb, our chairman, available.

We will close our markets on December 31st at 1:00 in the afternoon. We have that afternoon, that evening, and the entire weekend. The way we dispel the myths is that Monday at 9:30 a.m. the capital markets in the United States open and they trade.

Mr. TURNER. Thank you.

I think we might could sustain a run on the grocery store, Mr. Scher, but I do not think we could sustain a run on the banks or the security market.

Mr. SCHER. Well, as I said earlier, on behalf of the food industry, we have been in an offensive manner of working with our customers and our vendors ever since earlier this year. The food industry has done a very good job of communicating to the consumer that there is no need to panic. We are saying in ads and in a brochure, and the whole food industry is, if you are really worried, we advise you to stock up as if it were going to be a snowfall, no greater, no less. But if you are worried, get items like batteries and perishable and non-perishable items. Of course, the perishable items the day or so before, the non-perishable, we are telling people if you are really worried, you can stock up now. But we are telling people there is no reason to do so. We think we have done a good job of informing the public that you do not have to panic.

Mr. TURNER. Thank you. Thank you, Mrs. Morella.

Chairwoman MORELLA. Thank you, Mr. Turner.

Mr. Scher, you spoke on behalf of Giant Food. But how about other food distributors, are they in the same situation, do you know?

Mr. SCHER. The Ahold family, I mentioned earlier all the companies that are part of the Ahold family, over 1,000 stores along the East Coast. Dr. Tim Hammonds is president and CEO of the Food Marketing Institute, he has appeared before Congress, and I know that other food chains have also appeared. And the message has been one of that the industry has worked on the issue, that we are ready for Y2K, and we will, indeed, be ready. I might add that also goes for the vendors, the companies that supply the food retailers. We at Giant have contingency plans, but we also know that they have worked with other food chains around the country. So the manufacturers, the vendors, the people that supply us within the food industry, they are also ready.

Chairwoman MORELLA. Mr. Campbell, in your testimony you outlined some categories of potential Y2K events. I am curious about an example that you might want to give with regard to Y2K problems that would affect business processing and be visible to the public.

Mr. CAMPBELL. We start off with protecting our infrastructure and our technology with very basic starts, where all of our computer facilities, including the one in Rockville, are fully self-contained entities starting with the electric power. Our generator facilities have the capability of operating our operations stand alone.

Our biggest concern has always been the fear that people will make decisions about economics and buying or selling their securities based on a rumor. And it is our hope that our education has really been at the forefront and that people should not make economic decisions based on non-economic rumors or baseless fact.

We expect fully that all of our systems, we have done the end-to-end testing, we have contingency plans that have addressed every area that we can humanly comprehend or think up, we have prepositioned technology response teams across the country, and will do so. To our way of thinking, the worst part of any of the Y2K issues that we confront is the lack of investor education. And we continue to do that every day.

Chairwoman MORELLA. Where are you going to be on January 1, 2000?

Mr. CAMPBELL. I will be in my command center at K Street here. We will have a lot of our folks in Washington as well as both our primary and backup computer facilities in Connecticut and in Rockville.

Chairwoman MORELLA. Mr. Scher, are you going to be walking through the grocery store at that time?

Mr. SCHER. We will be ready.

Chairwoman MORELLA. Mr. Margolis, you mentioned that an inventory that had been done had something like 95 percent of the hospitals were compliant, but you assume there would now be more. Do you want to speculate on how many more? And of those that are not compliant, are they rural hospitals? And what will you do about that?

Mr. MARGOLIS. Thank you. I think they would not be differentiated as being just rural or just urban hospitals. The process of remediation with the thousands of medical devices is a process of working with vendors and testing equipment. And I feel confident that process continues to go on. Many vendors early on, and this is back in the spring of this year, were not even certain about their equipment and what impact it would have on Y2K. So that it took them some period of time to check with their own chip processors that made the embedded chips and the other circuitry contained within the equipment.

The remediation efforts are nearly complete. That 95 percent, which is actually more recently in our State of New Mexico 96 percent, is that equipment which has completely been remediated. And it is for that reason that I am confident that the remaining 4 percent is in the last few days of checking out and finally getting its Y2K compliance sticker, or that pieces of equipment that should not be used because it questionably may fail, it will be locked in a closet as not Y2K compliant and then could be pulled back out after January 1st.

Chairwoman MORELLA. And where are you going to be on January 1st?

Mr. MARGOLIS. Well, we have a command center in the hospital. It is a conference room with about 25 telephone lines in it which connects to the various departments. So I will not be partying. Maybe we will have some non-alcoholic punch available for 1 a.m. But in the Mountain States Time Zone we will be watching closely what happens here on the East Coast, and, of course, jointly with the AHA and the President's Y2K task force, we will be watching what happens to medical institutions and health care facilities in New Zealand, which is about 19 hours earlier than the Mountain States, should specific pieces of equipment be affected.

Chairwoman MORELLA. Thank you.

Mr. Willemssen, you have been very patient. I know that my time personally has elapsed, but I just wanted to quickly mention that I was alarmed when I read that in education 56 percent of the elementary and secondary schools in the United States were not compliant. I am just wondering what that can mean and what is it that we can do about it. This was like heating, security, telecommunications.

Mr. WILLEMSSEN. The education sector is one that you should be concerned about. Education has gotten a late start. As Mr. Koskinen mentioned, they have made excellent progress. But when your starting point is relatively so late, there really is reason for concern.

And one of the things that we have been emphasizing is the need for contingency plans for those educational institutions. Our survey of 25 of the largest school districts found many of them planning on December compliance dates. And as you know as well as anyone, information technology-related projects are often late. So that when you are planning on a December compliance date, it is going to be very difficult probably to make that date for all of those school districts.

So I think there is reason for concern. And I think it is therefore incumbent upon all of us to continue sounding the alarm for this

particular sector, as Mr. Koskinen and the Department of Education have done in the very recent past. That needs to continue.

Mr. MARGOLIS. Madam Chair.

Chairwoman MORELLA. Yes, Mr. Margolis?

Mr. MARGOLIS. Thank you. I just wanted to comment on higher education particularly as it pertains to medical schools. One issue has been, and we have talked about it collaboratively, the safeguarding of research projects, research specimens that are refrigerated that could be affected if power is lost. At most major academic centers, which certainly includes the University of New Mexico at this point, emergency power is in place to assure that both clinical laboratory specimens as well as long term research specimens, such as tumors, are under emergency power for continued refrigeration.

Chairwoman MORELLA. That just shows the tremendous implications that one has to think of. You cannot take anything for granted.

I am now pleased to recognize Mr. Bartlett.

Mr. BARTLETT. Thank you very much.

I do not know what the estimates are of the total amount that it has cost our country to get ready for Y2K. My question is, we knew a long time ago that this problem was coming. We started very late. Had we started in 1990 rather than in 1997 or 1998 or 1999, whenever we started, how much less in your judgement would we have paid to solve this problem? Obviously, the longer we waited, the more technology was there that needed to be fixed and assessed and it was going to cost more. How much less would it have cost us, you may give it as a percentage, in your judgement, if we had started this in 1990 rather than when we did?

Mr. MARGOLIS. Mr. Bartlett, I believe that the costs would probably be insignificantly less because in the case of hospitals, and I am sure in the case of financial institutions, there are so many interdependencies with other trading partners. Hospitals themselves could very well have upgraded their systems, checked their devices. But without input from the manufacturers of certain components, they would have been waiting until the present time until a lot of information was made available.

I think it is human nature to think of things in the future when the future gets a little closer. I speak from my own personal experience. I started out in computer programming and development myself in the 1970s and we talked many years ago about Y2K and no one believed that the computer programs that we were writing then would even be remembered by the time 1999 came along.

Mr. BARTLETT. But they have been remembered and we still use them. And when did we stop using a two-digit code in programming, which would tell you when the cost of fixing would be stabilized.

Mr. MARGOLIS. I could not answer that question directly. I know that at our hospital we stopped during the development of our current generation of client information systems. But I do know we have heard from other sectors that other software manufacturers have even introduced operating systems as recent as this year which had year 2000 defects. But they are easily correctable because they are upgraded with a later version of the software. That

is not to dispute why they were introduced as being deficient to begin with though.

Mr. BARTLETT. Which is the basis for my question. If starting in 1990 we had produced no programs with a two-digit date code, would not the problem have been a simpler fix?

Mr. MARGOLIS. I think it would have, but the interfaces between the systems would still be at issue. And in hospitals, that is the largest issue that we have. In our specific hospital, we have 80-some systems that speak to one another, that transfer data between one another. So it is not only the interface programs that hand off that data, but each of the programs that have to be Y2K compliant in the same way or in a way that you can understand so that the data is properly translated.

So that what you suggest would be the ideal. I am not sure that the cooperation of all the trading partners would have been achieved until the pressure of Y2K, the President's Council, and the Congress had been felt.

Mr. BARTLETT. Of course, if we had started with a four-digit date code, there would have been zero fix; is that correct?

Mr. MARGOLIS. That is absolutely correct.

Mr. BARTLETT. Okay. Mr. Campbell, our procrastination has cost us nothing?

Mr. CAMPBELL. Whenever you procrastinate, it costs you something. I would say that the greatest time that we have spent has been on our legacy systems, our older systems. As you build a one-of-a-kind computer system in the world and you start back many years ago, it is the legacy systems that take so much time to recertify. We would have also, Congressman Bartlett, had to certify all new systems that we put in place also. While it has cost us something, I think it is very difficult to place a percentage on it, and I do not think that percentage is a big percentage because of the integration testing and the certification of all systems across all vendors, across all different legacy and new systems. So even the systems that we put in today, we still make sure that we certify them as Y2K.

Mr. BARTLETT. Mr. Scher?

Mr. SCHER. Within the food industry, most major retailers started working on the problem 2 or 3 years ago. We do not believe there would have been significant cost-savings. Time is money, as they say, and there probably would have been some better flexibility with time scheduling in advance. But 3 years back the industry looked at the situation and worked aggressively, and the retail industry is ready.

Most people think of the food industry as a rather simple business—you go in, you buy groceries, you go home. Looking at what we have developed as far as contingency plans, it is mind-boggling. Things that we within the food industry, not just Giant Food, have had to be cognizant of include such things as advertising, direct store delivery, front-end operations, fuel operations, gas, getting products to our stores from our various vendors, perishables, areas of payroll, what happens if there is a power failure, if we cannot get store supplies, transportation, water and sewage. These are major issues that most people say, "Gee, I had no idea that is what was necessary to run a food store".

Again, I do not think it would have saved a great deal of money. Time, yes, if the industry would have worked a few years earlier. But, again, most retailers that I am familiar with have tackled the problem starting about 3 years ago in 1996.

Mr. BARTLETT. Madam Chair, I would like to ask Mr. Willemssen just a simple question.

Do you concur, sir, that the major liability that we have in starting late is that we might not finish rather than it cost us more?

Mr. WILLEMSSEN. I think the major liability is exactly that, that we may not finish in time. But I would also add that because we did get a late start, the pace, for all intents and purposes, was more frantic than it would have otherwise been. And you have to pay for that more frantic pace.

Speaking from the Federal Government perspective, the most recent estimate we have, the 24 major Federal departments and agencies, is about $8.9 billion that it will cost overall. One could argue that if that had been stretched out over a longer period of time, it may have been less. Indeed, there was a $3.35 billion emergency supplemental that was just for Y2K. One could argue that if the effort had been stretched out over time, agencies could have funded these activities through their normal budgeting process.

Mr. BARTLETT. Thank you all very much. Thank you, Madam Chair.

Chairwoman MORELLA. Thank you, Mr. Bartlett.

I am pleased to recognize Mrs. Biggert.

Mrs. BIGGERT. Thank you, Madam Chairman.

One of the rumors that I have heard lately, and I do not know if it is rumor, but so many of the hotel rooms in major cities have been booked, not for the celebrations of the turnover on New Year's Eve, but the fact that so many companies are having so many staff having to man the offices that they actually are having their families come into the cities and celebrate there because they will be involved with the turnover. Is that true, Mr. Campbell, from your standpoint?

Mr. CAMPBELL. We have scheduled, in Washington, 10 rooms at the Mayflower. We have scheduled rooms across the country because our staff needs to be there prior to the date, as well as the holiday traffic. So we have booked a considerable amount of room in the hotel industry around this country. You are absolutely right.

Mrs. BIGGERT. I think it will certainly be well-spent if we have those glitches that somebody will be there.

I would also like to commend you on your brochure and I guess this postcard. Is this something that was put into store bills, or is this something that was sent out through information?

Mr. CAMPBELL. It was sent out by our member broker-dealers across the country in the statements which they send to their customers every month.

Mrs. BIGGERT. Have you had response from the customers?

Mr. CAMPBELL. We have had quite an active session on our web sites with customers. And many of those customers would directly ask the broker-dealer that they deal with on a day-to-day basis many of the questions that they would ask us, and then we would respond either directly or to the member firms themselves. But our help desk has responded to over 20,000 requests over the last pe-

riod of time. So it has been very active, which is why we have really thought that education was probably the most important thing that we do.

Mrs. BIGGERT. I know one of the concerns about this has been fraud and that people were coming out with schemes to try and make money from this or take away money from people, particularly seniors, with scare tactics. Have you heard of anything where people have called your offices saying that somebody has tried to perpetrate something?

Mr. CAMPBELL. Not that I am aware of. The one issue that we have heard about is inducing people to withdraw money from their bank in cash form and then defraud them of that in one form or another. By and large, the securities industry is either book entry or by certificate, and the ability for somebody to walk into an office and demand ready cash is generally not the same as a bank.

Mrs. BIGGERT. And then Mr. Scher, I know that we have had concerns that there will be people who will decide at the last minute that they need to ensure that they have those supplies that they had not thought about until the last day or so. Do you think that still is going to happen? I do know that in a snow storm, coming from an area where we do have a lot of snow at that time of the year usually, that this happens—even in a major snow storm—where people rush to the grocery store at the last minute.

Mr. SCHER. We have extra merchandise that will be available in the stores and in our warehouses, both perishable and non-perishable, to ship. And we can do that in a matter of hours if need be.

I do not think you will be seeing that. Early in 1999, the news media was hyping this, and there was, indeed, a lot of interest on the part of consumers about what is going to happen. People were worried. We were getting dozens of media calls and consumer inquiries. Let's advance to November 1999. We are getting about six customer calls or letters a month, which is nothing, and all the news media calls to date have died down significantly. I think they will probably heighten slightly the last week of December.

But the message has changed from the news media's perspective, because of good reporting, to there is no need to panic. The message today is that the industry is ready. And that includes the banking industry that I have read about, the food industry, the airlines. So I think the apprehension on the part of the consumer is a lot less today than it was at the beginning of this year.

Mrs. BIGGERT. Good. Great. Thank you very much.

Thank you, Madam Chairman.

Chairwoman MORELLA. Thank you, Mrs. Biggert.

I am now pleased to recognize Mr. Ose.

Mr. OSE. Thank you, Madam Chair.

I first want to commend Mr. Scher's organization for this helpful pamphlet which on the back lists any number of web sites down at the bottom that folks can visit for additional information, and if they do not have access to the Internet, there is a phone number that they can call for information on this, a toll-free number, 888–USA–4Y2K. So my compliments to your organization for putting this together.

Mr. SCHER. Thank you.

Mr. OSE. I cannot let the occasion pass, Mr. Campbell, without expressing my compliments to you and your organization.

Mr. CAMPBELL. Thank you.

Mr. OSE. If I understand correctly from listening to each of you, the manner in which your business transacts is an increasing amount of its commerce is electronically. The hospital folks are ordering supplies electronically, you are exchanging shares electronically, you are buying food and produce electronically, probably paying your people electronically with direct deposit, et cetera. Each of those transactions goes over the telephone lines, in effect. It is a telephone conversation. Which brings me to my question, and I regret we do not have the opportunity to visit with someone today on that.

Mr. Willemssen, as far as the telephone companies, it is my understanding they are perhaps the most ready of all the various organizations in the country for this rollover.

Mr. WILLEMSSEN. I would probably not go along with they are the most ready. I am much more optimistic today than when I testified in the summer of 1998. I would continue to say that the banking and finance sector is probably the most ready. Within the telecommunications area, I think among some smaller local exchange carriers there is still some level of concern about their readiness. So bottom line for me on telecom, much more optimistic, but I would not put them at the absolute top of the heap.

Mr. OSE. Well, that brings me exactly to my question, and it relates primarily to Mr. Campbell's area of commerce. On Friday, December 31st, at 1 p.m., the exchanges are going to close, and at 9:30 a.m. on Monday, January 3rd, they are going to open. What is plan B if on Monday the 3rd there has been a problem?

Mr. CAMPBELL. Essentially, we operate one of the largest private communications networks that there is. We have paired T–1s to every server that we have across the country and across the world. All of those private, secure T–1 lines have been tested and tested and tested. The servers which they interface with have been tested. We have not only had physical on site presence to those servers, but the end-to-end testing that we have been involved in for quite some time leads us to believe that we know that our telephonic lines are operable in a Y2K environment.

We also have the ability to do many tests over that weekend, which we will. We do not quit testing. We do believe that the communications that transact share volume in the NASDAQ stock market are ready and operable, and will be, as they have throughout all of our end-to-end testing. We have transacted business coming in, we have compared trades, the clearing organizations have vented the transparency of that trade back out at the price that it took place. We have gone through the order entry, to the transaction, all the way through the settlement and clearing process in a year 2000 environment, having rolled on numerous times our calendars forward.

We believe that we are ready. If we have issues to deal with, we will deal with them. But we believe that with the integrated testing end-to-end that we have done, we are ready and we will be ready.

Mr. OSE. Thank you.

Chairwoman MORELLA. Thank you, Mr. Ose.

It is now my pleasure to recognize the co-Chair of the House Working Group on Y2K, the gentleman from California, Mr. Horn.

Mr. HORN. Thank you, Madam Chairman.

Let me start with NASDAQ. It established a record high, as we all know, surpassing 3,000 in closing yesterday. And technology stocks really dominate that board. Last week, IBM announced that mainframe computer customers are waiting to buy new equipment until after January 1st as they grapple with their own Y2K problems.

What is the danger that Y2K could adversely affect the stock exchanges and investors' interests?

Mr. CAMPBELL. First of all, I think that whenever you approach year end, you either speed up your purchasing or you delay your purchasing, depending upon where you are with your budgets or the issues that you are dealing with. We do that at NASDAQ and I know the Federal Government does that. Essentially, in IBM's case, I believe that it was a postponement, obviously, is what you said, and deferral of major purchases while they concentrated on making sure they were Y2K compliant.

The SEC has been very diligent in requiring the disclosure of the Y2K risk that firms have. They have gone back and back, and those firms they felt had not been as forthcoming as they would have desired, they have gone back to them and asked them for more specificity with respect to their risks. I think that the technology companies are more aware of Y2K and as sophisticated in the remediation because they are either the problem or they have been the solution. So relative to the damage that it would pose across the country, I think that it will be very limited in scope.

Mr. HORN. In terms of contingencies, what things do you have on Y2K problems that affect businesses? What is the contingency plan?

Mr. CAMPBELL. Our contingency plan deals with many different levels of issues; whether or not somebody has telephone issues, whether or not they have order entry issues, whether or not they can operate their systems. We have it tiered in many layers. We have very specific reporting requirements over the weekend from December 31st to January 3rd. Those very specific reporting requirements go to the different capital markets and the regulators. The Securities and Exchange Commission has very specific reporting requirements over that weekend. We will be, and have been, linked in terms of all the communications that will take place.

So there are checklists for as many contingencies as our creative minds have been able to think up over the last couple of years. They are quantified, they are in books, they are in our command centers. We practice, we will continue to practice, and we will have basically triaged as many different contingencies and unexpected kinds of issues that we know how to create.

Mr. HORN. A number of us have said from the very beginning that this is a management problem, not just a technological problem. What have you learned out of this experience that might be useful should some similar circumstance ever occur? It might be the encryption bit and how little bright kids break through computer security and all the rest of it.

Mr. CAMPBELL. We deal with security issues every day. From a management perspective, my best training is probably as an Air Force pilot and knowing what to expect that nobody has ever trained you for. Essentially, not only from our web sites, but our private communications systems, to our computers, to our people issues, I think that it has continued to make us more aware that it has to be done on every facet every day from a security perspective. So I think that it has been, at least from my perspective, a very broadening experience. Hopefully, I have learned something from it.

Mr. HORN. Would any of you other witnesses like to comment on that? What have you learned from this that might be worthwhile knowing as a management problem when we ever get into something like this again? It obviously will not be this particular thing, hopefully, but it could be other things that relate to computers.

Mr. SCHER. That is a very good question, Mr. Horn. We are looking at Y2K as an opportunity. We think we will not miss a heartbeat; it will pass us by. But your question is a good one. In the event of a natural disaster within the food industry, let's take just one segment, people on welfare, people who receive Government benefits from the State and Federal levels, if the phones go down, for example, people that are on the electronic benefit transfer program, which is almost throughout the United States today, they would go into a food store and not be able to access their benefits.

So what have we learned? We have learned that, aside from Y2K, we should indeed have good contingency plans in the event of, for example, telephones go out. A large segment of our customer base would not be able to shop for something they need to survive—food. So we have to look at alternative plans to handle a situation if, for example, the telephone lines go down again, how do we serve that customer. It is a question that we discuss today with one of our other owners, one of the other members of the Ahold family, Giant Food Stores of Carlisle, and we do not have the answer. It is a very good question. Aside from Y2K, if the phone lines go down, how do we serve this important segment of our business. We are going to be addressing that also.

So it has widened our horizons. It has opened our eyes to look at possible other disasters that could occur within a retail business, how do we solve those problems. Some of those solutions are inherent with what we have found out with Y2K. Others we will be exploring over the next few months. But it has, indeed, opened our eyes to potential other disasters that could occur.

Mr. HORN. Would cellular phones be one of the options for your major customers, a direct line?

Mr. SCHER. Possibly. If phone lines go down and a welfare individual or family is in a food store, they are at the checkout, we would have—currently, if the computer does not work today, we have a number that we can call within the State government to make sure that the benefits or their so-called account has funds in it. A cellular line would work perfectly for that. It is a little cumbersome, but we would have to resort to something other than telephone lines and that is what we would use.

Mr. HORN. Mr. Scher, in terms of the food situation, is there a concern within the food retail distribution industry about transpor-

tation being available to get the products you need on a regular basis? I assume a lot of the stores use what we call the Japanese inventory approach; on a timely basis, it gets there based on the demand. Is there going to be stockpiling in some cases in the back of particular stores if they do not have the space?

Mr. SCHER. Mr. Horn, for certain commodities within the food industry, yes, the food stores, to the best of their ability, have small back rooms that they will stock up with extra merchandise. Our warehouses will also have certain items that we know that, for example, if there is a snow storm, people would normally buy, including such items that are non-perishable like batteries, candles. We will have our truck fleet standing by. In the event that we see panic buying occurring, we will be able to ship merchandise to the stores. But with certain commodity groups, we will have excess product in the store just to be safe.

Mr. HORN. Let me ask the gentleman from New Mexico. I have long admired the medical school at the University of New Mexico. I am curious, they were the ones that in the freshman year of medical school mixed the students studying medicine with actual patients, and not just the dull bio-chem or whatever courses, anatomy, so forth, but relating them to real human beings. Is that still going on at New Mexico?

Mr. MARGOLIS. Yes, sir, Mr. Horn, it does. It is the encounter or problem-based medical training. They were pioneers in that area.

Mr. HORN. Well they were No. 1, but Harvard got the publicity because it is Harvard.

Mr. MARGOLIS. I am glad that story has travelled back east.

Mr. HORN. And having headed a State university and been a head of a lot of those people, but you never get publicity because you do not have 35 people on your staff.

Mr. MARGOLIS. That is right.

Mr. HORN. So I was just wondering if that kept going, because I have had a great respect for that institution for 20 years.

Mr. MARGOLIS. I will let the dean know. He will be very glad to hear that.

Mr. HORN. Well, it is a very interesting situation. Let me ask you, with the AHA, when we were in Cleveland the representative of the Cleveland Clinic, a very distinguished group of hospitals, was our witness and noted that there was a common web site where you could check out the equipment as to machine number, patent, and all of the rest of it and you did not have to reinvent the wheel if you were checking your various pieces of equipment in the emergency room. Has that worked pretty well? And has the hospital profession been able to get and share information with each other so they do not have to reinvent the wheel?

Mr. MARGOLIS. Yes, that has worked very well. Actually, through the leverage of the State Hospital Associations and the American Hospital Association, we have shared a lot of information like that. The FDA, as you know, has a site for medical devices where you can check serial number, manufacturer, and other information to rely upon the piece of equipment being tested by the manufacturer, which is often the safest reliance you can have.

In addition, the American Hospital Association has put together a monthly telephone conference line, one for rural hospitals and

one for large urban hospitals, where on a monthly basis for the last 11 months we have shared information regarding what we have found with our vendors, what we have found in our own institutions, and how our remediation plans have been going, which has been an excellent forum for learning from one another and avoiding that issue of reinventing the wheel. So, although in many ways we are competitive with other hospitals in our community, it is important to share certain levels of data because we are community service-based providers and it is critical that we be able to respond as a team and not as a single hospital island.

Mr. HORN. Now a lot of the manufacturers of some of that emergency equipment probably were out of business. Did you find there were ways to get replacements for some piece, or did you just have to go and let's buy something new?

Mr. MARGOLIS. In some cases. I can think of three or four pieces of equipment, and that was I believe EKG pieces of equipment, that had to be replaced because the manufacturer had in fact been out of business for something more than 10 or 12 years and there was no successor to that manufacturer that could provide the upgrade. The reality is a piece of equipment like that has a useful life of 8 to 10 years. So, on the one hand, it was probably time to replace it, but, as you know and commented about New Mexico, we probably did not have the money to budget to replace it and so we would have liked to have kept it running. But, for the most part, there has been successor companies who are able to provide the upgraded software, and in many cases the upgraded computer processing board, which will allow that piece of equipment to operate beyond January 1st. Most of that was done under warranty or maintenance service agreements that we have.

It is a large challenge for hospitals to have identified all that. But that is part of their remediation plan and, as you pointed out, much of that information has been shared over various web sites.

Mr. HORN. Now in going through this exercise, which nobody wanted obviously to do, but you had to do it for your own computer systems, have you learned something that will help you in better arranging new computers which are needed in terms of a new generation? We are always out; the minute we have bought one, it is 3 years out of whack anyhow. But what have we learned from that in terms of did we need all those programs, could you get rid of some, could you merge some? Did anybody use that as an exercise to say why are we doing this?

Mr. MARGOLIS. I think a valuable lesson that we have learned is the compatibility between equipment and the need when procuring equipment or software, which is mostly what hospitals do rather than develop their own software, to use common standards in data communication to insist that vendors can provide that common interface. There are committees of HCFA I believe that have defined something called HL–7, which is a standard of data interface, and that has become very popular in the last 2 years, to insist that vendors provide software that can communicate using this HL–7 interchange. I think that is probably the most valuable lesson because that will ensure not only for year 3000, which is quite a distance off, but for various things that happen in terms of Federal programs and insurance programs, that various pieces of the data

process share the same codes for the same meaningfulness of the data.

Mr. HORN. The way you are getting the new replacements for some of us, we might be around in the year 3000.

Mr. MARGOLIS. I hope I am.

Mr. HORN. You gentlemen really did a great job and in your written presentations. I think it is one of the best panels we have ever had before us. It was very useful as to what you have gone through.

I am going to ask Mr. Willemssen, who has followed us everywhere in the United States, overseas, you name it, and we usually ask him, because he has got all this knowledge, to say what have we missed. And what would you suggest? Ask some questions that make sense to you.

Mr. WILLEMSSEN. I think you have really touched on some of the key points that you would want to hear from these witnesses. The only thing that I might add from a lessons learned perspective that maybe these sectors have learned, that we have definitely learned in the Federal Government, is going into this, and going into future information technology problems such as this, you need to focus on the business function first and the system second, instead of thinking systems and then how do they work for the business. That is one lesson learned in the Federal Government is focusing on the programs and then looking at the supporting systems rather than the other way around.

Mr. HORN. Anybody want to add something that came to mind that we did not ask you? This is your chance.

[No response.]

Mr. OSE. Mr. Chairman, I have one thing I want to make sure that Mr. Scher addresses, because come January 1st, if there is not an adequate supply of Oreo cookies in his store, he is going to have trouble.

Mr. SCHER. They will be there, I promise you.

Chairwoman MORELLA. You are talking to a Marylander, we believe in the Oreos, however you spell it.

Mr. HORN. Well, if the Chair would indulge me, there is a few closing remarks I would like to make that I did not make because I was not here. I was in a markup of my subcommittee earlier.

Chairwoman MORELLA. Mr. Chairman, before you make the closing remarks, may I just ask one other question. We are also going to open it to members of the committee of both subcommittees to be able to present any other questions to you, if that is amenable.

But I just had a question that dealt with an article that I saw in USA Today. It was an article that indicated that a number of companies have failed to comply with SEC regulations requiring full disclosure of a company's vulnerability to Y2K. I just wondered if any of you wanted to comment on is this a widespread problem? Does this imperil investor confidence? Because I think it would affect all of you and I just wondered if you wanted to make any comment on that.

Mr. CAMPBELL. It is my understanding, Madam Chair, that it is a very small contained group of companies that the SEC has gone back and asked for further information. Obviously, the most important thing that the management of a company can do is maximize

and protect their shareholder value. And those companies that do not have full disclosure obviously risk that.

Chairwoman MORELLA. Anyone else, because it actually would affect all of you.

Mr. SCHER. No problem.

Chairwoman MORELLA. Are you okay with, I know NASDAQ is going international, but the Asian markets, the interoperability concept?

Mr. CAMPBELL. We are moving forward relative to globalization of our markets. The links at this present time do not provide major risk to the U.S. capital markets. Essentially, we will know early whether those markets operate, how they operate. But the connection between the markets is not there at this point in time. So at least to U.S. citizens, the issue relative to their domestic securities is not at issue, it is their foreign owned securities. We have not had any direct conversation with the foreign markets except in terms of exchanging information about Y2K from a technology perspective. So I really cannot address that.

Chairwoman MORELLA. If there were a run on the Asian markets and you found out before it happened here, how would you react?

Mr. CAMPBELL. I think our reaction would be to address the confidence issue in our domestic markets. I think all of our markets, all the regional markets, the national exchanges would address those in concert along with the SEC. The most important facet, we believe, of our markets is there is confidence in them; they are well-regulated, they are transparent, and they do protect the investor. That happens no where else in the world like it happens here. So we would address that very openly and very directly and we would share with the investing public exactly what is happening.

Chairwoman MORELLA. Mr. Willemssen, do you want to comment on that issue at all?

Mr. WILLEMSSEN. We have not done an analysis of that particular issue, so I am not in a position to comment.

Chairwoman MORELLA. Thank you. I want to thank all of you, too.

Now I am going to defer to Chairman Horn, the co-Chair.

Mr. HORN. Thank you very much, Madam Chairman.

No one really knows what is going to happen on January 1 and December 31 in terms of what happens when we switch over. We have got predictions that are springing up like wild flowers about this. We have eager entrepreneurs promoting their year 2000 survival kits. We have some of the people in the county jail have already talked to the warden and the captain of the guard to say could you let me off for December 31st and January 1st because they think everybody will take money out of the bank and put it in their homes. That is the stupidest thing an American citizen or anyone here could do is take money out of the bank and put it in their homes because that is just where the robbers and burglars and all the rest of them will be looking.

Already, I read into one hearing a letter to Ann Landers on the scams already happening to elderly citizens. And all I can say is it needs to be "buyer beware" in those last few days in terms of people selling you things you really do not need. A lot of them just might collapse on you anyhow. I have been looking at probably 100

different magazines over the last couple of weeks and have seen these ads that are the kinds of things you would see in the National Inquirer or something that want to scare your wits out of you. But we do have some real problems.

Of course, some of this is just amusing in a way, but it certainly is upsetting people. For example, in 1993, Minnesota officials instructed 104-year old Mary Bandar to report to kindergarten. Now it turned out that the State computers had misread Ms. Bander's 1889 birth date as 1989, placing her at age 4. Recently in Maine, several hundred car owners were dismayed to find the titles to their new year 2000 model vehicles categorized as "horseless carriages." State computers has misread the year 2000 as 1900.

Well, we can get by those things. But some of the more serious ones obviously worry us; and that is, how you get gas from Russia to Eastern Europe, Central Europe, would that affect the United States in any way? Will the electricity fail? So forth. Now both the administration and the Congress have looked at a number of these questions around the country and I think people have been very prepared. When we had a problem on nuclear reactors, we asked the Nuclear Regulatory Commission to look at all of them, not just 10 percent; they were only going to look at 10 percent. They have looked at all of them and presumably that situation which generates electricity is okay. But we really will not know until you get it all in an operational sector where you have all of these different factors coming together in a typical operational day. And that is the main thing we really have to care about.

We will have two more things in terms of these two subcommittees. One, we will hold the final grade release to the press on November 22nd, a Monday, and the staffs and the GAO team that has worked very closely with us will be doing the work of analysis that week. We think that should tell us a little bit about at least the executive branch. I think Mr. Koskinen and his team have done a fairly good job. The question is could it all have been done earlier, and would it have cost less. We still have shades of panic even in the executive branch as well as in private industry when a lot of their talented people have been bought out from under them by other industries who want talented people. The question will be did we have enough human resources in the right place at the right time. Again, that is a management question.

So, Madam Chairman, I think we hope you will be there on November 22nd. And then your committee and mine, after this is all over, we will have a retrospect summing up, and if something has gone wrong, what could we have done to get the administration to do it the right way then. I was worried for several years over the procrastination. I think they have played catch-up and I hope they make it. That is what we need. We should not have to do things that are just fouled up and not run on a steady track of some sort of management approach to solving the problem.

And so that is where we are. We do not know what is going to happen on January 2nd and December 31st. But you certainly give us some heartening hope in major industries that you represent, the hospitals, the grocery industry, the stock markets. I know the stock markets were one of our first witnesses when we started and I think they have done a splendid job. So thank you all for coming.

Mr. HORN. Mrs. Morella, I think we have the tributes to the staff.

Chairwoman MORELLA. And as he gives the tributes, I want to indicate that I would agree that the cost has escalated, maybe it would not have had we started earlier. I remember the first submission by the President was $2.3 billion. Remember that, Mr. Willemssen? Now it is $8.9 and probably continuing. But we will be continuing to monitor, and we appreciate very much your being here and for your patience for being here all afternoon.

Mr. HORN. I might add that the GardnerGroup, when they testified before our subcommittee, said it will be about a $30 billion cost in the case of the Federal Government. We think, and we thought as it went along, and we simply pulled it out of the air, but that is the way they sometimes build budgets around here, we thought it would be $10 billion. And that is about where it is I believe.

So we are going to thank our staff that has stuck with this now since 1996. Russell George, the staff director and chief counsel, is standing against the wall there. Don't worry, we are not some Latin American banana republic where people that stand by walls are in trouble. You are in good shape. Matt Ryan, senior policy director, is right behind me here. Bonnie Heald, communications director, is probably working with the press. Chip Ahlswede, our clerk, is right there with them. Rob Singer, the staff assistant; P.J. Caceres, intern; Deborah Oppenheim, intern. That is all of our staff.

And then Mrs. Morella's staff of the Subcommittee on Technology of the Science Committee: Jeff Grove, the staff director; Ben Wu, behind us, counsel; Joe Sullivan, staff assistant.

The minority staff on the Government Management, Information, and Technology Subcommittee team is Trey Henderson, minority counsel; Jean Gosa, the minority staff assistant. On the Technology Subcommittee, Michael Quear, the professional staff member; and Marty Ralston, staff assistant. And the court reporter is Ruth Griffin.

We thank them all for all they have done. They have worked overtime many a night, many a weekend to get the job done, and we appreciate it.

Chairwoman MORELLA. We will now adjourn the committee meeting.

[Whereupon, at 5:07 p.m., the subcommittees were adjourned, to reconvene at the call of their respective Chairs.]

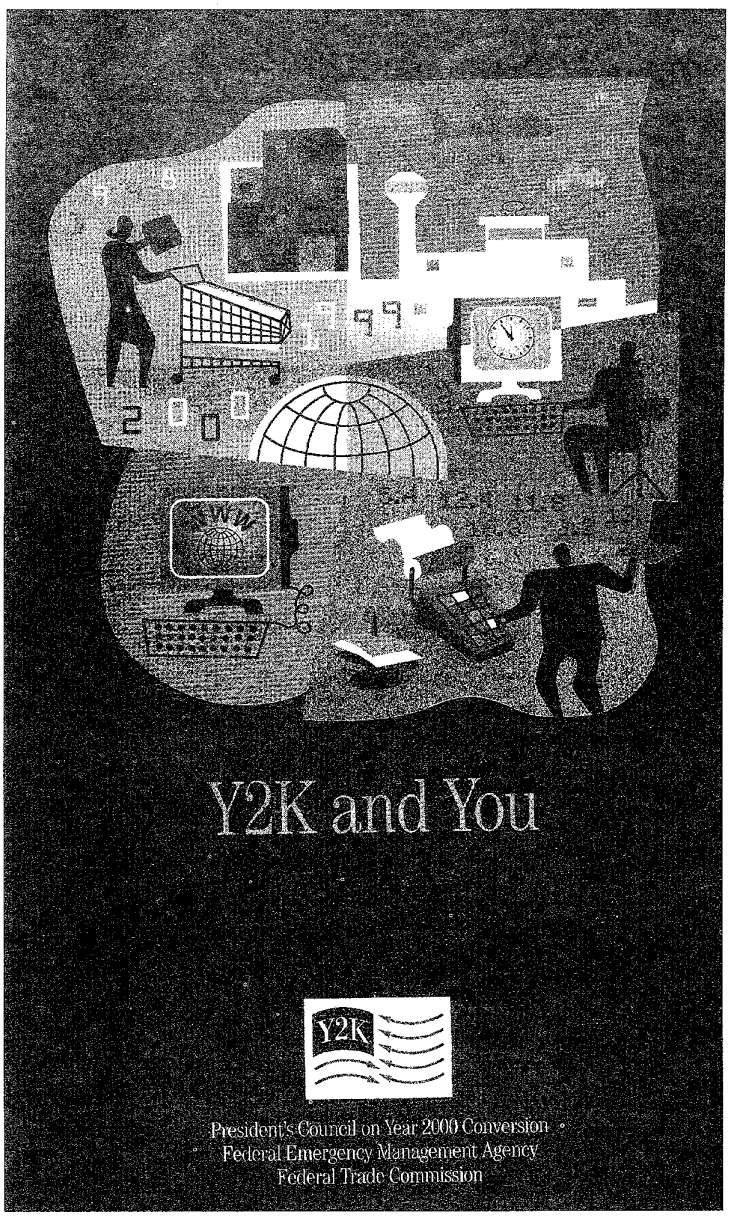

Y2K and You
Y2K
President's Council on Year 2000 Conversion
Federal Emergency Management Agency
Federal Trade Commission

Table of Contents

Y2K

This booklet offers background information on the Y2K issue and provides suggestions on how you and your family can prepare for the century date change.

WHAT IS THE YEAR 2000 ISSUE?

The Year 2000, or Y2K, issue (also known as the Y2K problem, the Y2K Bug, and the Millennium Bug) refers to the difficulty some computers may have telling the difference between the Year 2000 and the Year 1900. Computers not able to properly recognize the Year 2000 date may produce incorrect data or shutdown.

While it is unlikely the Y2K issue will affect most of the appliances and electronic equipment we use in our homes, the large number and inter-connectivity of computers we depend upon every day make Y2K a serious challenge. In the workplace, computers help to operate everything from factory production lines to cash registers. As a result, businesses and governments in the United States have spent billions of dollars over the past few years to make sure their computers will be ready for the date change.

How Did It Happen?

In the early days of computers, computer memory was scarce and expensive. Computer programmers saved memory space by using two digits to represent the year. For example, 1999 was entered as "99." Over time, the use of two digits became common within the computer industry and, today, a number of computers operate with this format. When the Year 2000 arrives, not all of these computers and electronic systems will be able to properly recognize the new year.

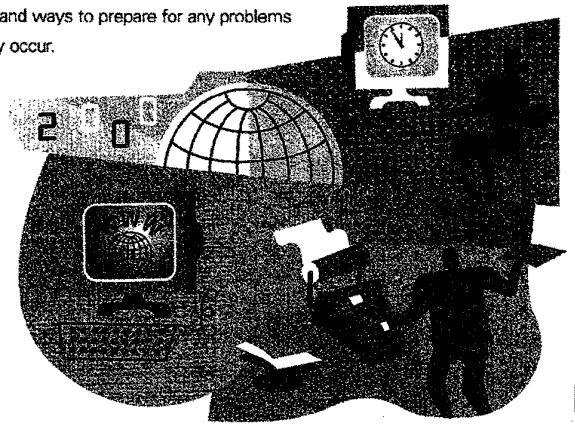
61-629 00 - 7

Does the Y2K Issue Apply Only to January 1, 2000?

Some people think the Y2K issue will surface only on New Year's Day. This is not true. Y2K challenges can happen any time a computer that is not Y2K compliant uses a Year 2000 date. A number of businesses and governments have already had to use Year 2000 dates in their automated operations. Hotels and airlines operate systems that have been processing Year 2000 reservations for several months. Many companies and government agencies have budget systems in which Fiscal Year 2000 has already begun and they too have been operating successfully. On the other hand, some glitches or problems caused by the Y2K issue may not be apparent for several days or weeks after January 1, 2000.

Somebody told me... I heard that...

A great deal has been written and said about what could happen on January 1, 2000. Some of it is true, but a number of the stories and tales told about Y2K are not accurate. This booklet is designed to provide you facts about the Y2K issue, what it could mean to you, and ways to prepare for any problems that may occur.



HOW WILL THE Y2K ISSUE AFFECT ME?

Outside the home, we all rely on companies and other organizations in our communities for important services (e.g., electric power, telephone service, banking). Many organizations have made a significant effort to prepare computers for the date change and test back-up plans in case there are system failures. But no one can say for sure that there won't be problems or glitches related to the Y2K issue. These problems could create temporary disruptions in some services.

Information provided to the President's Council on Year 2000 Conversion and the public indicates that the major national systems that support the basic infrastructure in the United States (e.g., networks for power, telecommunications, transportation, financial transactions) are expected to be ready for the Year 2000. There is, however, significant concern about smaller organizations that are taking a "wait and see" approach to the Y2K issue (i.e., wait to see what breaks and fix it after January 1). This concern particularly applies to some small businesses, local governments, health care facilities, and educational institutions.

Organizations taking a wait and see approach to the Y2K issue are placing themselves — and the people they serve — at a greater risk of experiencing difficulties related to the date change.

What Should I Do?

It is important for individuals, like businesses and governments, to be prepared for Y2K. You can use the information provided in this booklet, along with Y2K readiness information from your local service providers, to help you and your family to be ready for the date change. We encourage you to follow the steps outlined

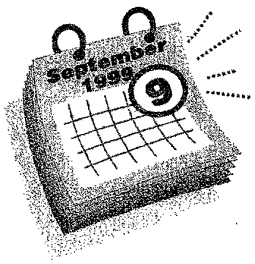
in the Y2K Preparedness Checklist (pages 16-17) to be better prepared for Y2K or any future emergency.

If you have additional questions about the Y2K issue, the Federal Government operates a toll-free Y2K information line – 1-888-USA-4-Y2K (1-888-872-4925). The line is operational 24 hours a day, seven days a week, with updated information on the most requested subjects. Information specialists and researchers are available to answer your questions during normal business hours, Monday - Friday. You can also call the information line to order additional free copies of this booklet.

For More Information

★ The President's Council on Year 2000 Conversion web site — http://www.y2k.gov — contains regularly updated information on the Y2K issue and links to other important Y2K-related sites. The President's Council, which was created by President Clinton in February 1998, is in charge of coordinating the Federal Government's Year 2000 efforts. Information on the web site is also available by calling 1-888-USA-4-Y2K.

Did You Know?
9/9/99
The 9/9/99 date milestone (consecutive "9s" were sometimes used as a command to stop computer programs) passed with only a handful of reported glitches, but it is no reason to become complacent about the Year 2000. The Y2K issue is a different, and more widespread, challenge for computers.



UTILITIES

We rely on local utility companies every day for power, phone service and water. These companies have been working diligently to make sure that they are ready for the Year 2000, so that on New Year's Day people can enjoy the normal festivities of the holiday season.

Electric Power

The electric power industry has completed most of its Y2K remediation work and is confident in its ability to make a successful transition to the Year 2000. While the possibility of local power outages can never be ruled out — there are no guarantees any of us will have power tomorrow, let alone on January 1 — the industry is accustomed to planning for and responding to outages caused by bad weather, accidents, equipment failures, and other events.

Telephone Service

It is unlikely the Y2K issue will create difficulties for the nation's telecommunications network. Large telephone companies, which provide services to most Americans, have been leaders in fixing and testing systems to make sure they are ready for the Year 2000. The major U.S. local and long distance carriers expected to complete upgrades of their key systems by the end of September 1999.

Telephone usage is expected to be heavy on January 1, 2000. People are encouraged to use telephones, and the Internet, only as necessary on New Year's Day. "Testing" the systems to see if they work or engaging in long conversations could create delays greater than those experienced during high volume usage periods such as Mother's Day. If you are unable to obtain a dial tone, it is

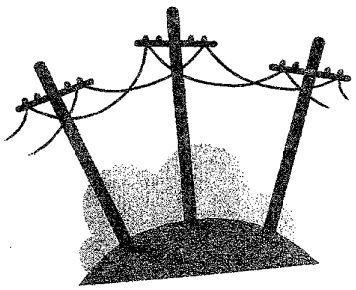
recommended that you wait several minutes before making another attempt to place your call or to log on to the Internet.

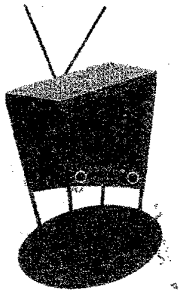
Water

Water system operators are confident that they will be ready for the date change. Most of them are fixing and testing their automated processes. In the event of problems, most facilities can convert to manual operations as a back-up.

For More Information

- ★ Read utility company notices about Y2K readiness. If you have additional questions, contact your individual service provider. You should be able to find contact phone numbers on your most recent bill.
- ★ The Federal Communications Commission web site — http://www.fcc.gov/year2000 — contains information about the Y2K preparations of the communications sector.





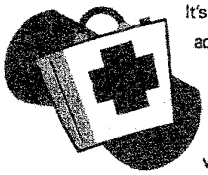
Did You Know?

Television and Radio

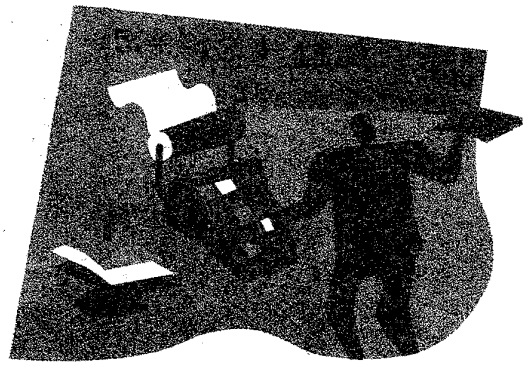
Broadcasters have been taking steps to ensure that the Y2K issue will not affect radio and television broadcasts. The Federal Communications Commission is confident that, even if some broadcasters experience service outages due to Y2K-related problems, the multiplicity of listening and viewing options ensures that there is little risk the public will be without radio and television broadcasts as a source of information.

Did You Know?

Personal Preparedness



Disruptions in basic utilities can happen at any time. It's always a good idea to make sure that you have adequate clothing, tools and supplies, flashlights, batteries, a battery-powered radio, and a first aid kit, as recommended by FEMA and the American Red Cross. For more information, visit: http://www.fema.gov/pte/emprep.htm and http://www.redcross.org/disaster/safety/emerprep.html, or call FEMA at 1-800-480-2520.



PERSONAL FINANCE

Across the United States, people make an annual estimated 1.8 trillion retail purchases using credit cards and engage in 11 billion transactions using automatic teller machines (ATMs). Computers are an important part of these and other activities involving your finances.

Banks, brokerage and securities firms, and other financial institutions are among those that have received the highest marks for Y2K readiness. In addition to devoting years of effort and spending billions of dollars to make sure their own systems are ready, financial institutions have been cooperating with one another to test the points where computers interact throughout the industry.

Your Money

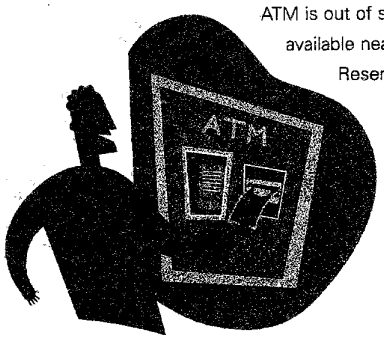
It is extremely unlikely that the Y2K issue will cause banks and other financial institutions to lose track of your finances. Financial institutions have been working for years to make sure that computers used for record keeping will be ready for the Year 2000 and most financial institutions are required to keep back-up copies of critical books and records stored in electronic form.

Depository institutions such as banks, thrifts, and credit unions have extensive Y2K programs in place. Federal financial regulatory agencies like the Federal Reserve, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency have conducted multiple examinations of their progress and have found that virtually all Federally insured depository institutions are ready for the date change.

The securities industry, under the supervision of the Securities and Exchange Commission (SEC), has been working aggressively to make sure that the Year 2000 will mean business as usual for its operations. Firms are required to report to the SEC on their Y2K readiness. The roughly 400 broker/dealers, markets, and clearing and settlement organizations that clear all market transactions participated in detailed industry-wide Y2K testing in spring 1999. The testing produced very few Y2K glitches, and those that did occur were fixed quickly.

ATMs

Depository institutions and firms that operate ATM networks have established aggressive programs with rigorous testing to make sure that ATMs will work normally on January 1 and every day thereafter. While most ATMs are expected to make a successful transition to the new year, remember that temporary disruptions in ATM service are not unusual and may not be Y2K-related. If one ATM is out of service, another one is usually available nearby. In addition, the Federal Reserve has taken steps to make sure that financial institutions have sufficient cash available at year's end.



Credit Cards

Credit card companies are confident that their key systems will be ready for the Year 2000 and, with retail stores, are making sure individual credit card processors are ready as well. As always, stores that experience difficulties with their automated credit processing equipment can process card transactions manually.

Reported problems about the use of credit cards with post-1999 expiration dates appear to have been solved. Most consumers have now successfully made purchases using credit cards with expiration dates in the Year 2000 and beyond.

Employer Payroll and Retirement Plans

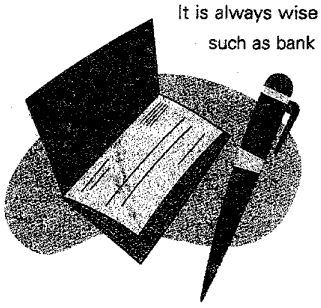
Your employer should be making sure that computer systems for payroll and retirement funds are ready for the date change. If your employer has not provided you with information about Y2K efforts in these areas, it is a good idea to inquire about their readiness.

For More Information

- ★ Make sure to read Y2K notices from your bank and other financial service providers.
- ★ The Federal Financial Institutions Examination Council web site — http://www.ffiec.gov — provides additional information about financial institutions' Y2K readiness.

Did You Know?

Financial Records



It is always wise to keep copies of important records such as bank and financial statements. When you receive a transaction receipt, check it for accuracy and save it to compare against your statement.

Did You Know?

Cash

Withdrawing large amounts of cash for Y2K is unnecessary and may invite theft. If you decide to withdraw cash, hold only as much as you would for any holiday weekend. Remember that, as always, you have more than one payment option (e.g., checks, credit cards, debit cards, traveler's checks).

Did You Know?

Scams

Beware of Y2K scams. Be skeptical if someone tries to sell you a product, service or investment that is "Y2K safe" or wishes to sell you Y2K insurance. Never give out your bank account, credit card or Social Security number unless you initiated the call or contact.

FOOD AND FUEL

The food industry has been focused on making sure its computers will not be affected by the Y2K issue. Food manufacturers, distributors, and supermarkets report that, as a result of these efforts, consumers will find that stores have ample supplies of essential food and groceries.

Food

Grocery stores are already anticipating a surge in sales at the end of the year because of millennium celebrations, and they intend to have sufficient inventory on hand. The nation's supermarket companies report that they normally have five weeks of inventory in their distribution centers and stores. These stocks provide a supply cushion in times of unusual demand surges.

If supermarket companies do experience Y2K-related difficulties, it is important to remember that the industry is accustomed to operating under adverse conditions. Companies already have contingency plans in place so that they can continue to serve their customers when, for example, bad weather creates problems with power and other services.

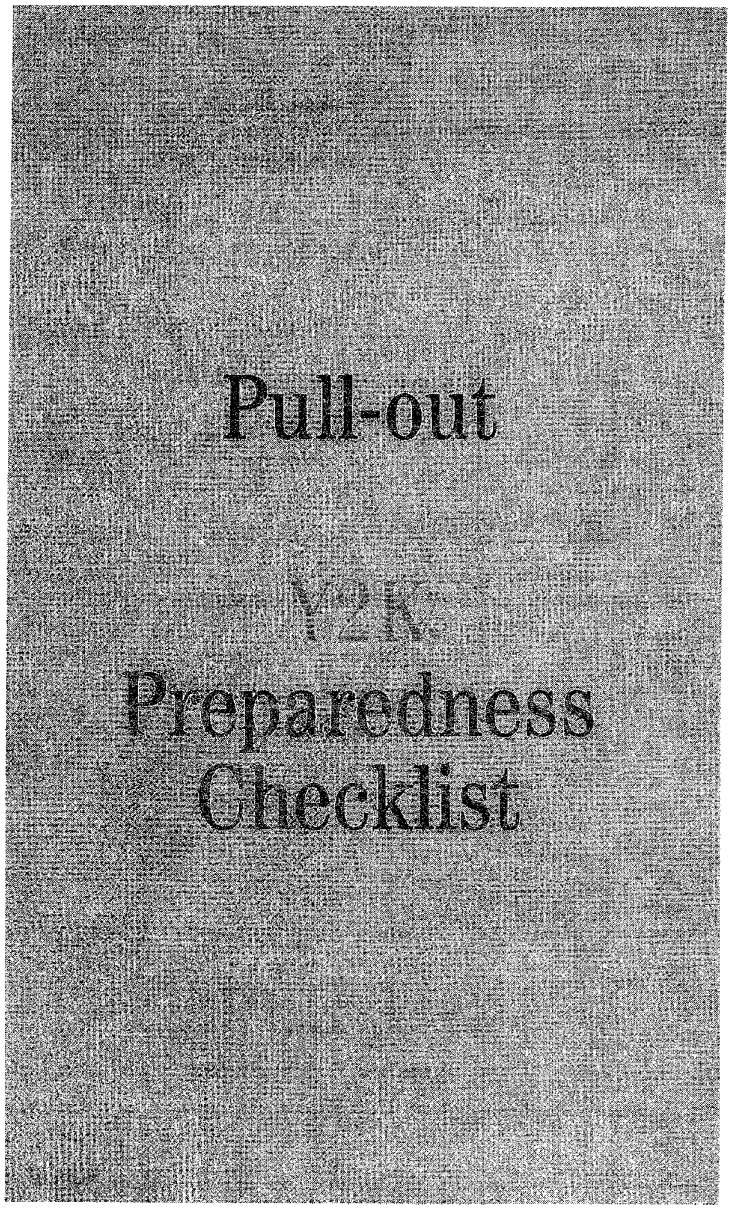
Gasoline

The oil and gas industry expects to conduct business as usual over the New Year's weekend. The industry is committed to ensuring safe and reliable delivery of gasoline in the Year 2000 and beyond. Service stations have been testing and, when necessary, replacing fuel pump systems to make them Y2K-ready.

Home Heating Oil and Natural Gas

Supplies of home heating oil and natural gas should not be affected by the date change, according to the oil and gas industry. Companies have been checking and testing embedded systems found in pipelines carrying petroleum and natural gas, as well as in drilling platforms and rigs. As the New Year approaches, the industry is advising consumers to arrange for regular delivery of heating oil.

While there are concerns about the Y2K readiness of some developing countries from which the United States imports oil, two of the major suppliers to the U.S., Canada and Mexico, are basically done with their Y2K work.


Pull-out
Y2K
Preparedness
Checklist

Y2K PREPAREDNESS CHECKLIST

Governments and businesses have spent billions of dollars to ensure that computer systems will make a successful transition to the next century. Although it is unlikely that the Year 2000, or Y2K, issue will create significant problems in the United States, no one can say for sure that there won't be temporary disruptions in some services. Such interruptions are expected to be short-lived, like temporary problems in service caused by storms, and while inconvenient, are not expected to cause long-term problems. The following recommendations will help you and your neighbors prepare for any difficulties that may occur:

❑ **Local Information:** Read Y2K notices provided by local government officials, banks, power and telephone companies, health care organizations and other important service providers. Adapt the recommendations in this checklist to what you learn locally and to your past experiences with local service providers.

❑ **Food, Water and Other Supplies:**

✓ Prepare as you would for a long holiday weekend by having at least a three-day supply of food and water (one gallon per person per day). The food industry is not only ready for Y2K, but it is resilient and accustomed to dealing with unexpected disruptions (e.g., storms). As always, it is a good idea to make purchases early.

✓ Make a personal assessment of items and services that are critical to your family, including special items or services required by family members with special needs, such as infants, the elderly and persons with disabilities.

✓ Make sure that you have adequate clothing, tools and supplies, flashlights, batteries, a battery-powered radio and a first aid kit, as recommended by FEMA and the American Red Cross. For further information, visit: **http://www.fema.gov/pte/emprep.htm** and **http://www.redcross.org/disaster/safety/emerprep.html**, or call FEMA at **1-800-480-2520**.

✓ Follow all appropriate safety instructions for fuel storage and use of heating and cooking devices or other emergency items.

❑ **Important Records:** Keep copies of important records — particularly your bank and financial statements, medical records and prescription drug information — in the few months before and after January 1, 2000. When you receive a transaction receipt, check it for accuracy and save it to compare against your statement.

✓ Develop a list of phone numbers for hospitals, police and fire departments and neighbors.

❑ **Cash:** If you decide to withdraw cash, hold only as much as you would for any holiday weekend. Withdrawing large amounts of cash is unnecessary and may invite theft. Remember that financial institutions are well prepared for the date change and you have more than one payment option (e.g., checks, credit cards, debit cards, traveler's checks).

❑ **Medicine:** As always, refill prescription medications when you have a five- to seven-day supply remaining. The pharmaceutical and health care industries are confident, based on experience, that following this standard practice is all that is needed for Y2K. If you have any questions about your health care needs, talk to your doctor, pharmacist or other health care provider.

❑ **Gasoline:** As you would in preparation for a winter storm, keep your automobile gas tank above half full. Service stations are re-supplied regularly — sometimes as often as every other day.

❑ **Consumer Electronics:** Check with manufacturers to see if the essential electronic equipment you use around your home is Y2K ready, especially personal computers, monitored security systems or programmable thermostats.

❑ **Telephones and Internet:** Use telephones and the Internet only as necessary on January 1. "Testing" the systems to see if they work or engaging in long conversations could create delays greater than those experienced during high volume usage periods such as Mother's Day.

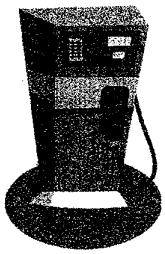
❑ **Scams:** Beware of Y2K scams. Be skeptical if someone tries to sell you a product, service or investment that is "Y2K safe" or wishes to sell you Y2K insurance. Never give out your bank account, credit card or Social Security number unless you initiated the call or contact.

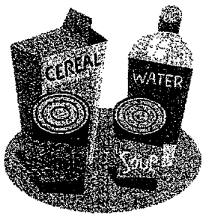
For More Information

- ★ Many grocery stores have brochures and other written materials about their Y2K readiness. If you are interested in learning more, ask for a copy during your next visit.
- ★ The U.S. Department of Agriculture's web site — http://www.usda.gov/aphis/FSWG — contains additional information about the Y2K readiness of the food supply system.
- ★ For more information about the Y2K readiness of the oil and gas industry, visit the Council's Oil and Gas Sector Working Group web page at http://www.ferc.fed.us/y2k/index.html.

Did You Know?
Gasoline

Gasoline service stations are re-supplied regularly — sometimes as often as every other day. Nonetheless, you should always keep your automobile gas tank above half full.





Did You Know?
Food and Water

Since no one can say for sure that there won't be some Y2K glitches, prepare as you would for a long holiday weekend by having at least a three-day supply of food and water (one gallon per person per day). As always, it is a good idea to make purchases early.

HEALTH

In health care, making sure that computers are ready for the Year 2000 is an important priority. Most hospitals, doctors offices, health clinics, and long-term care facilities across the United States have been working together to identify and solve potential date change problems.

Large health care facilities have aggressive efforts underway to make sure the Y2K issue will not affect their operations. However, much less is known about the readiness of smaller health care providers. Y2K difficulties are not expected to have a direct impact upon patient care, but record keeping and payment systems could be at risk in health care facilities taking a wait and see approach to the Y2K issue.

Hospitals

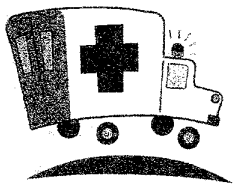
Most hospitals have contacted local medical vendors, suppliers, and other organizations to make sure that hospital medical devices, as well as important record keeping and payment systems, are ready for the Year 2000. As an extra precaution, hospitals are also updating long standing back-up plans for storms and other events so that they can continue to provide health care in the event of temporary disruptions in key services such as power and telecommunications.

Medical Devices

Medical devices include a wide range of equipment used in hospitals, ambulances, and long-term care facilities. Medical devices also include implanted items, such as pacemakers, but these are not affected by the Y2K issue.

The U.S. Food and Drug Administration has requested that medical device manufacturers assess whether their equipment is Year 2000 compliant. Manufacturers have discovered that some devices may experience minor problems related to the Y2K issue, such as showing an incorrect year date on display monitors. The vast majority of medical devices do not have date change issues that will affect patient health or the delivery of safe and appropriate care.

Health care facilities are dedicated to making sure that the few devices that rely more extensively on computers — and could present problems for patient care if not fixed before December 31, 1999 — receive appropriate upgrades or are replaced.



Home Health Care

Medical devices and equipment used in home health care are not likely to experience Y2K problems that will affect their safe operation. It is a good idea, however, to contact each item's manufacturer to make sure that it will function properly in Year 2000 and beyond.

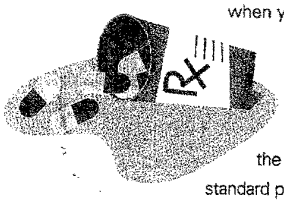
For More Information

- ★ If you have concerns, ask your doctor or local health care facility about their readiness for the Year 2000.
- ★ For more information on medical devices and the Y2K issue, visit the Food and Drug Administration's web site at http://www.fda.gov/cdrh/yr2000/year2000.html.

Did You Know?

Prescription Medications

It is always a good idea to refill prescription medications when you have a five- to seven-day supply remaining. The pharmaceutical and health care industries are confident, based on experience and the 90-day supply of finished products in the supply system, that following this standard practice is all that is needed for Y2K.



Did You Know?

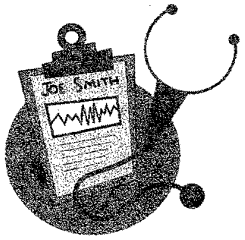
911 Systems

The organizations responsible for the operation of 911 answering centers vary by community. Some are operated by fire departments, others are run by police or private companies under contract to the local government. If you wish to find out more about the Y2K readiness of your local 911 systems, check with your local emergency services office.

Did You Know?

Medical Records

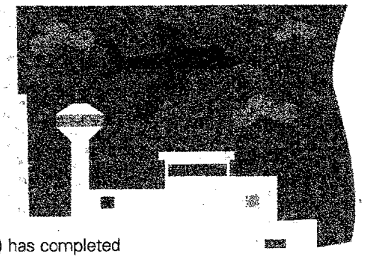
Keeping copies of important records such as medical histories and prescription drug information makes good sense for Y2K or any other time.



TRAVEL

The travel industry faces a global challenge with the Y2K issue. If you stop for a moment to think about travel outside the United States, it isn't hard to imagine how many computers play an important role in your safe transport and comfortable stay abroad.

The travel industry — including airports, airlines, government aviation officials, and travel agents — for some time has been fixing and testing systems within the United States so that they will be ready for the Year 2000. Overseas travel authorities are also making sure their systems are ready, but much work remains to be done on the Y2K issue in a number of countries. If you have plans to travel outside of the United States during the New Year's holiday, especially to developing countries, you should expect some difficulties related to the Y2K issue.



Domestic Air Travel

The Federal Aviation Administration (FAA) has completed work to make sure that all of its systems — including those involved in air traffic control — are fully compliant for the Year 2000, and it is updating back-up plans just in case there are system problems.

The FAA has also been engaged with airlines, airports, and airplane manufacturers to make sure the Y2K issue will not affect the safety and effectiveness of their operations and products. Airplane manufacturers report that they have not found any Y2K problems in aircraft that would present a safety risk to passengers.

Travel Outside the United States

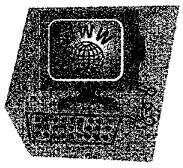
While many countries have made extraordinary progress on the Y2K issue in the past year, concerns still exist about Y2K readiness in some parts of the world. Individuals with plans for travel outside the United States can obtain country-specific information on Y2K readiness abroad from the State Department's Bureau of Consular Affairs and the Department of Transportation.

For More Information

- ★ The State Department provides country-specific information to travelers through consular information sheets and, in some cases, travel warnings. Consult http://travel.state.gov/y2kca.html or your travel agent for more information.
- ★ The Federal Aviation Administration web site — http://www.faay2k.com — contains information about the FAA's preparations for the date change.
- ★ The Department of Transportation web site — http://www.fly2k.dot.gov — provides information about the Y2K readiness of international aviation systems.

Did You Know?

Travel Information



The State Department has for some time provided Americans traveling or living abroad country-specific information through consular information sheets on more than 180 countries. These sheets have been updated to include information on country Y2K readiness. You can consult http://travel.state.gov/y2kca.html for more information about these resources.

AROUND THE HOME:
DOMESTIC APPLIANCES, CONSUMER ELECTRONICS, PERSONAL COMPUTERS, ELEVATORS

Items With No Significant Risks

Most appliances and consumer electronic systems in use around the home do not keep track of the year date to operate effectively and will probably not be affected by the Y2K issue. Refrigerators, ovens, microwaves, coffee makers, television sets, smoke detectors, washers and dryers, and alarm clock radios should not have difficulties with the date change.

In addition, major auto manufacturers that account for roughly 90 percent of all cars and light trucks sold in the United States have stated that the Y2K issue will not affect the safety and performance of their vehicles. If you have questions about a specific vehicle, contact the manufacturer or your local dealer.

What May Be Affected

A small number of domestic appliances and other consumer electronic systems are "year-date aware" and may experience Y2K-related difficulties. While it is unlikely that such difficulties will cause these products to stop working entirely, they could create inconveniences and should be checked. As always, it is a good idea to contact the manufacturer if you have any questions about whether a specific product will be affected by the Y2K issue.

VCRs

While most VCRs will not be affected by the Y2K issue, some models manufactured before 1987 that program by calendar date may experience difficulties.

Y2K problems with these few older VCRs will not disrupt your ability to play videotapes or view television programming if you use the VCR tuner to change stations on your TV set. However, timed recording could be affected. If you have an older model VCR and want to find out whether it is Y2K ready, contact the manufacturer.

Calendar Programmable Thermostats

Some home thermostats with advanced calendar functions that allow consumers to program temperature settings months in advance could be affected by the Y2K issue. If you have such a thermostat, contact the manufacturer to determine whether it is Y2K ready.

Security Systems

Professionally installed home security systems and home safety systems connected to large commercial monitoring systems should continue to operate normally in the Year 2000. However, small, consumer-installed systems may experience Y2K-related problems.

Consumers with questions about their security systems should contact the manufacturer. If you own a system that is connected to a professional monitoring service, it is also a good idea to find out if that company's systems are ready for the date change.

Cameras and Camcorders

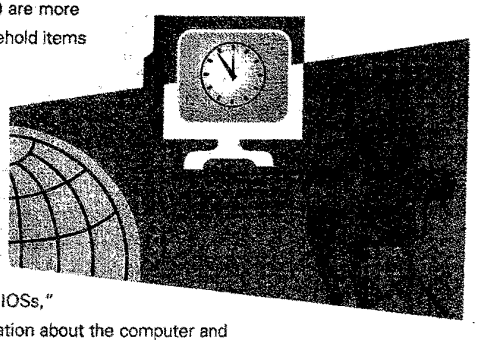
Most cameras and camcorders that are date-aware will recognize the Year 2000 without difficulty. However, models that have problems recognizing the year will still work but may display the wrong date. Manufacturers can provide details on how to reset calendar date displays.

Fax Machines

Some fax machines that are not Y2K compliant may be unable to initiate and receive a call or fax. It is a good idea to check with the manufacturer to determine whether your machine is ready for the date change.

Personal Computers

Personal computers (PCs) are more complex than other household items and are at greater risk of experiencing Y2K-related difficulties — in hardware, operating systems, and software.



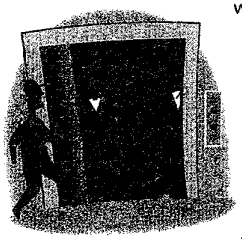
Hardware in PCs could be vulnerable to the Y2K issue. In particular, PC "BIOSs," which store basic information about the computer and access its electronic calendar, could be affected. Operating systems (e.g., Windows 95), including some introduced as recently as 1998, could also experience problems related to the date change.

Software used for word processing, graphics, and games will probably not be affected by the Y2K issue. Software used for applications where year dates are critical, such as in spreadsheets, money management and personal organizer programs, could have problems and needs to be checked.

Most computer and software manufacturers offer extensive information about how the Y2K issue could affect their products. Fixes, or "patches," can often be downloaded from the Internet. Check manufacturer web sites for more information.

Elevators

If your apartment or condominium building is equipped with an elevator, you should know that many elevator manufacturers have said their products will not be affected by the date change. Otis Elevators, one of the largest manufacturers, reports that its elevators are not year-date dependent.



It is important to note, however, that elevators could be affected if they are tied into larger building-control systems that are not Y2K ready. If you live in a building where you depend upon elevators, check with the building manager or community association to make sure they are on top of the situation.

Global Positioning System Receivers

Global Positioning System (GPS) receivers — often used for navigational purposes by recreational hikers, boaters, and campers — could be affected by the Y2K issue, which may result in users receiving incorrect navigational data. If you own a GPS receiver and want to find out whether it is ready for the Year 2000, check with the manufacturer.

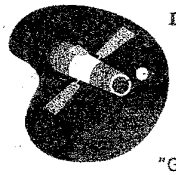
For More Information

- ★ Many consumer electronics companies, PC manufacturers, and software companies have made information available about the Y2K readiness of their products. Check their web sites or call their toll-free information lines for details.
- ★ The PC Y2000 Alliance web site — http://www.pcy2000.org/testing/index.htm — contains links to Y2K web sites for PC manufacturers, steps to conduct manual tests, and links to free automatic tests.
- ★ The Federal Government's consumer web site has a Y2K section — http://www.consumer.gov/y2k — that contains Y2K compliance information for personal computers, consumer electronics, and automobiles.
- ★ Check http://www.navcen.uscg.mil/gps/geninfo/y2k/default.htm (the Coast Guard Navigation Center's web site) or call 1-888-USA-4-Y2K to find out more about how to contact GPS receiver manufacturers.

Did You Know?

Building Operations

You may live in a building where you share access to heat, power, and telephone service with other residents. If you do, it is a good idea to check whether your building manager or community association has taken steps to make sure these systems are ready for the date change.



Did You Know?

Global Positioning System

While many Global Positioning System (GPS) receivers passed an August 21 date challenge (the so-called "GPS End-Of-Week rollover") without difficulty, users should still check with manufacturers to make sure their receiver is ready for the Year 2000.

THE FEDERAL GOVERNMENT: GETTING READY FOR Y2K

The Federal Government has undertaken a massive effort to ensure that its thousands of computer systems, which help to provide services to millions of Americans, will be ready for Year 2000.

Agencies have been working for years — some, like the Social Security Administration, since 1989 — to make sure that systems are ready for the date change. They've been evaluating systems, fixing or replacing those that are not Year 2000 ready, conducting system testing, and developing and testing contingency plans.

As a result of this major effort, the Federal systems and processes that help to provide some of the most important government services — from Social Security and veterans benefits to air traffic control, Medicare, and weather forecasting — are ready for the date change.

Federal agencies also monitor the administration by State governments of a number of important Federal benefit programs including Food Stamps, Child Nutrition Programs, WIC, Medicaid, Temporary Aid for Needy Families, Child Support Enforcement, Low Income Housing Energy Assistance Program, Child Care, Child Welfare, and Unemployment Insurance.

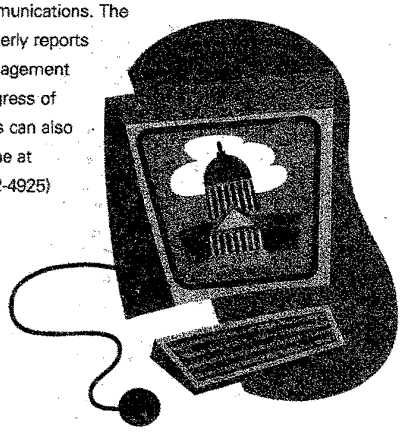
Some States do not expect to finish their Y2K work on State-administered Federal programs until late 1999. If you depend upon these programs and have questions about your State's Y2K readiness, contact your State program office.

President's Council on Year 2000 Conversion

The President's Council on Year 2000 Conversion was established in February 1998 to coordinate the Federal Government's Year 2000 efforts. The more than 30 agencies represented on the Council are committed to making sure that Government systems and programs will make a successful transition to the new century.

The Council's working groups, led by Federal agencies, have been encouraging others — including businesses, State, local, and tribal governments, and other countries — to ensure that the Y2K issue does not affect their operations. Industry trade associations have been major partners in the Council's efforts by increasing awareness and gathering information about how their members are addressing the Y2K challenge.

The Council maintains a web site at http://www.y2k.gov that contains the most recent information about the Y2K issue, including the Council's quarterly status reports on Y2K within major industry sectors such as electric power, finance, and telecommunications. The web site also contains quarterly reports from the U.S. Office of Management and Budget on the Y2K progress of Federal agencies. Individuals can also call the Council's toll-free line at 1-888-USA-4-Y2K (1-888-872-4925) for more information about the Y2K issue.



This consumer information pamphlet is offered at no cost by the President's Council on Year 2000 Conversion. For additional free copies, contact the Y2K toll-free hotline at 1-888-USA-4-Y2K.

---

www.y2k.gov
President's Council on Year 2000 Conversion
1.888.USA.4.Y2K